NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

INFORMATION SECURITY REQUIREMENTS FOR A COALITION WIDE AREA NETWORK

by

Susan C. McGovern

June 2001

Thesis Advisor: Cynthia E. Irvine
Second Reader: Orin E. Marvel

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2001	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Title (Mix case letters) Information Security Requirements for a Coalition Wide Area Network			**5. FUNDING NUMBERS**
6. AUTHOR(S) Susan C. McGovern			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

To achieve information superiority in a coalition environment the U.S. has to seamlessly integrate coalition members, both NATO and Non-NATO, into its command and control processes along all echelons of military operations. In a coalition environment, it is extremely challenging to fuse multinational information systems to achieve seamless integration. This thesis focuses on the security issues that are involved in establishing coalition network interoperability. The coalition environment is defined in terms of purpose, command structure, mission area, and control functions. Network and information protection are discussed in terms of minimizing the threats to information systems security. Coalition information system user requirements are defined and some of the security mechanisms required to meet those requirements are discussed. Current solutions to secure coalition network interoperability are surveyed, followed by conclusions, recommendations and areas for further study.

14. SUBJECT TERMS Battlespace Environment, Command, Control, and Communications (3), and Information Assurance			**15. NUMBER OF PAGES** 98
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

INFORMATION SECURITY REQUIREMENTS FOR A COALITION WIDE AREA NETWORK

Susan C. McGovern
Lieutenant, United States Navy
B.A. Political Science, University of California at Los Angeles, 1992

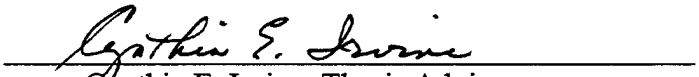
Submitted in partial fulfillment of the
requirements for the degree of

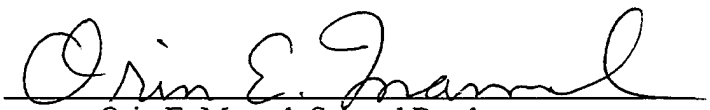
MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY (COMMAND, CONTROL, AND COMMUNICATIONS)

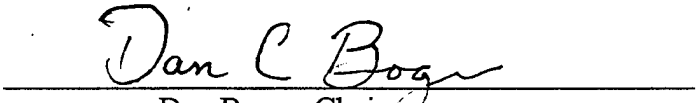
from the

NAVAL POSTGRADUATE SCHOOL
June 2001

Author: 
Susan C. McGovern

Approved by: 
Cynthia E. Irvine, Thesis Advisor


Orin E. Marvel, Second Reader


Dan Boger, Chairman
C3 Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

To achieve information superiority in a coalition environment the U.S. has to seamlessly integrate coalition members, both NATO and Non-NATO, into its command and control processes along all echelons of military operations. In a coalition environment, it is extremely challenging to fuse multinational information systems to achieve seamless integration. This thesis focuses on the security issues that are involved in establishing coalition network interoperability. The coalition environment is defined in terms of purpose, command structure, mission area, and control functions. Network and information protection are discussed in terms of minimizing the threats to information systems security. Coalition information system user requirements are defined and some of the security mechanisms required to meet those requirements are discussed. Current solutions to secure coalition network interoperability are surveyed, followed by conclusions, recommendations and areas for further study.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The characteristics of warfare evolve overtime. Change occurs as a result of the effects technological breakthroughs have on tactics and doctrine. Typically, advances in military technology are employed sparingly on the battlefield, until the full potential of the technology is realized, and usage becomes widespread, evolving beyond the original design and intended use of the technology. History provides several examples of how the use of new technology shifted the fundamental means of conducting warfare. At the turn of the last century, mechanized vehicles replaced mounted cavalries; the success of the aircraft carrier in World War II shifted the center of naval warfare from battleships to carriers; and within the last fifty years, advances in weaponry, radar, and the ability to control the electromagnetic spectrum have enabled the strike air campaign to replace ground or amphibious assault as the predominant means of projecting power. In all cases, the technology preceded the shift in tactics and doctrine.

Technologic advances have increased the area of warfare operations. Over one hundred years ago, the area of operation was limited to the reach of command and control functions such as bugle calls, telegraph, and horse-bound messenger. As advances in mobility, weaponry and communications evolved, the ability to project power expanded to regional, continental and now global proportions. The means to project that power is harnessed in Command, Control, Communication, Computer and Intelligence (C4I) systems. These systems enable warfighters and decision makers to establish a simultaneous virtual presence anywhere in the battlespace. For example, the President of the United States can be briefed, using information systems such as Video-

teleconferencing, on an emergent crisis situation, be apprised of military assets in the area, presented with alternative courses of action, decide upon and order an air strike to target a specific location; all while en route via helicopter or Air Force One to Middle East peace negotiations.

The expanse of the battlespace, declining military budgets and the existence of a common powerful adversary motivate nations to form military coalitions. U.S. strategic doctrine and future vision reflect a preference to conduct military operations in a coalition environment. Actions of an aggressor nation can have far reaching effects within a region or even the world. Often these nations are too powerful to be defeated by a single nation without weakening that nation significantly in the process resulting in a change to the balance of power in the region. By sharing the burden of military action, regional stability can be achieved more quickly and less expensively in terms of lives, and economies. In the court of world opinion, a coalition of nations acting to curb aggression provides legitimacy to that action. Coalition action is based on consensus of all participating nations. Building that consensus is one of the challenges of coalition warfare.

Coalition warfare is very complex because of language and cultural barriers, differences in training, doctrine and tactics, and national laws and regulations regarding foreign command and control of national forces. Technical incompatibilities and national laws and regulations regarding the sharing of sensitive military information create communication problems. The combined power of a coalition requires strong coordination and control mechanisms. The lives of each nation's members depend on interoperable communications; therefore, finding a means to resolve these

communication interoperability problems is essential. The notion of protecting information according to policy using sound network security mechanisms predates the Internet. Although connectivity is a concern, technologies exist to meet the connection needs of the coalition. The key factor required to facilitate data communication is adequately and properly protecting the information that is being shared. This requires implementation of security practices and policies within the coalition wide area network. The correct implementation of security mechanisms and policies will ensure information confidentiality, integrity and system service availability. Protecting the information transiting a wide geographic area on a heterogeneous network is a complex task. This is the environment of the coalition wide area network. A geographically distributed network composed of "come as you are" hardware and software from the various member nations.

In recent coalition military operations, Bosnia and Kosovo for example, nations would establish their own national local area networks (LAN) to process the intelligence, tactical data and planning documents required in military operations. Data that was required to be shared among coalition members would be air gapped from one LAN to another through the use of floppy disks and runners, uploaded, worked on, and then air gap returned with modifications, deletions or approvals. There was no assurance, save that of the personal integrity of the runner, that the information that left one area was delivered to the other without modification or unauthorized disclosure. Moreover, the information was downgraded to the lowest releasibility level common to the entire coalition.

B. PROBLEM STATEMENT

A coalition wide area network must be developed to meet the Coalition Task Force Commander's operational needs while maintaining the security goals of information confidentiality, integrity, nonrepudiation and system service availability. This system should operate within a heterogeneous environment with multiple levels of security available at one workstation (workspace real estate is a premium). This thesis will identify the Coalition Task Force Commander's network operational needs and address the means to provide them in a secure and efficient manner.

C. APPROACH AND SCOPE

A combination of literature review and personnel interviews was conducted to ascertain the network operational needs of the Coalition Task Force Commander. Based on these requirements security solutions are identified and explained. Finally, current technologies being considered or used as solutions to the coalition network security problem are reviewed and assessed with regard to their advantages and disadvantages.

D. OVERVIEW OF REMAINING CHAPTERS

Chapter II provides a broad overview of coalition operations with regard to its purpose, composition, command and control structures and functions, missions and the special challenges associated with the coalition environment.

Chapter III provides an overview of basic network security. System protection mechanisms and concepts are identified and explained. The specific challenges to network security in the coalition environment are then discussed.

Chapter IV introduces the Coalition Task Force Commander's network operational needs and discusses the security mechanisms and policy implementation required to meet those needs.

Chapter V discusses current technologies being deployed, in testing, and in proof of concept development. Each is designed to meet one or all of the Coalition Commander's network security needs.

Chapter VI summarizes the research, provides conclusions, recommendations and suggests areas for further research and study.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. PURPOSE OF A COALITION

Operating within a coalition is a concept that is as old as the history of man. A coalition is a union of persons, statesmen or political parties to achieve a specific objective. This discussion uses the term coalition to refer to a combination of two or more multinational military forces. Therefore anytime man has combined his power with another against some common enemy or in support of some common cause, a coalition was formed. The United States was founded based on a coalition of commonwealth statesmen against the tyranny of King George III of England. In the broadest sense of the word, the American Revolution was fought between two coalition forces – the United States and France against the British and German Hessian soldiers.

One would think that a nation borne of coalition blood would be steeped in the practice of coalition warfare. Such is not the case. From the end of the Revolutionary War until its entrance into World War I, the United States preferred national isolation to forming coalitions. Again, in 1942, it was an act of war that roused the U.S. from its isolationism to participate in yet another coalition. However, since World War II, U.S. tactics, doctrine and policy have emphasized a preference to conduct military operations within a coalition environment.

With the end of World War II, the U.S. was thrust into the role of "Leader of the Free World". Given its foundation in democracy and national characteristics of fairness and amicability, coalition building is a natural inclination and preferred method of leadership. There are several reasons for building and joining coalitions.

1. Legitimacy

Building a coalition against a common enemy or cause lends legitimacy to that cause. While the U.S. is positioned to take unilateral action to counter any threat, acting in concert with other nations validates that action in the court of international opinion. International consensus also facilitates majority approval from the U.S. Congress.

2. Shared Risk

In periods of peace, national governments and citizenry demand justification for placing military men and women in harms way. This is especially true if the proposed action is perceived as outside the vital interests of a nation. The idea of shared risks encourages cooperation from national governments and peoples.

Shared risks also imply shared responsibilities. In a coalition each nation assumes tasks and responsibilities commiserate with their military capabilities. Many nations cannot muster the military might necessary to bring a crisis to a favorable end. In this instance, sharing the risk with an ally or friendly neighboring state can result in achieving the desired end state.

3. Declining Defense Budgets

National defense budgets declined significantly with the ending of the Cold War. As nations began to reduce the size of their forces, their ability to project power unilaterally diminished as well. Therefore, the need to form coalitions to counter aggression or ensure peace has become imperative. In fact, members of the North Atlantic Treaty Organization (NATO) base their defense spending on the premise that real world operations will be undertaken in conjunction with the U.S.

4. Rapid Response

Future regional aggression is likely to occur far from U.S. territory. Allied and friendly nations joined in a coalition may act as a rapid response force to contain aggression while the U.S. mobilizes and deploys its forces. [Ref. 1]

B. COALITION COMPOSITION

The composition of modern coalitions is dynamic. Membership within a coalition may change from day to day, certainly from coalition to coalition. These dynamics are driven by national politics. If a coalition engages in a course of action outside the express national interests of a member nation, that nation is entitled to break with the coalition. The ad hoc nature of a coalition precludes the formal and binding agreements, such as treaties, that exist among members of an alliance. As a result, nations are free to come and go in accordance with national goals and objectives. Each member nations' motivations are different. These motivations will be self-serving. For example, many low technologically developed nations join coalitions to gain the experience of operating with technologically advanced nations. Coalitions are composed of several actors: national political and diplomatic envoys, military professionals, representatives of Non-Government Organizations (NGO) such as the United Nations; members of Private Voluntary Organizations (PVO) such as Doctors Without Borders; and Public Affairs Organizations (PAO) such as the Cable New Network. A universal thread among coalitions is that once the common goal for which it was formed has been accomplished, the coalition dissolves.

C. COALITION COMMAND AND CONTROL

Command and control is the exercise of authority by a properly designated commander over assigned forces in the accomplishment of the mission [Ref. 2]. Coalitions are created to quickly respond to unexpected crises that are beyond the bounds or scope of unilateral or alliance action. Therefore, command relationships evolve as the coalition is formed. [Ref. 3 p.II-11] Each participating nation's force commander is instructed by its national authority on the desired end-state to be achieved. That end-state is the basis for formation of the coalition and is the common thread that weaves the coalition together.

1. Command and Control Structure

Successful military operations start with a command structure designed to inspire unity of command. History provides numerous examples of the failure to implement unity of command. During the World Wars, the mode of command chosen to instill unity was the appointing of a Supreme Allied Commander. This individual wielded the consolidated combat power of several nations. Over the past 50 years the style of warfare has changed and with it, the organizational structure of the command element. In recent coalition operations, the structure of command has taken three shapes: parallel command, lead nation command and a combination of the two. In addition, the emphasis on unity of command has shifted to emphasize unity of effort.

a. Parallel Command

In many instances political tensions or national law forbid the subordination of one nation's military to another nation's command. As a result, a

parallel command structure with no single commander is adopted. Here unity of effort is achieved through careful coordination. This is the most fragile and ineffective means of coalition command and control. Figure 1.1 shows a parallel command structure

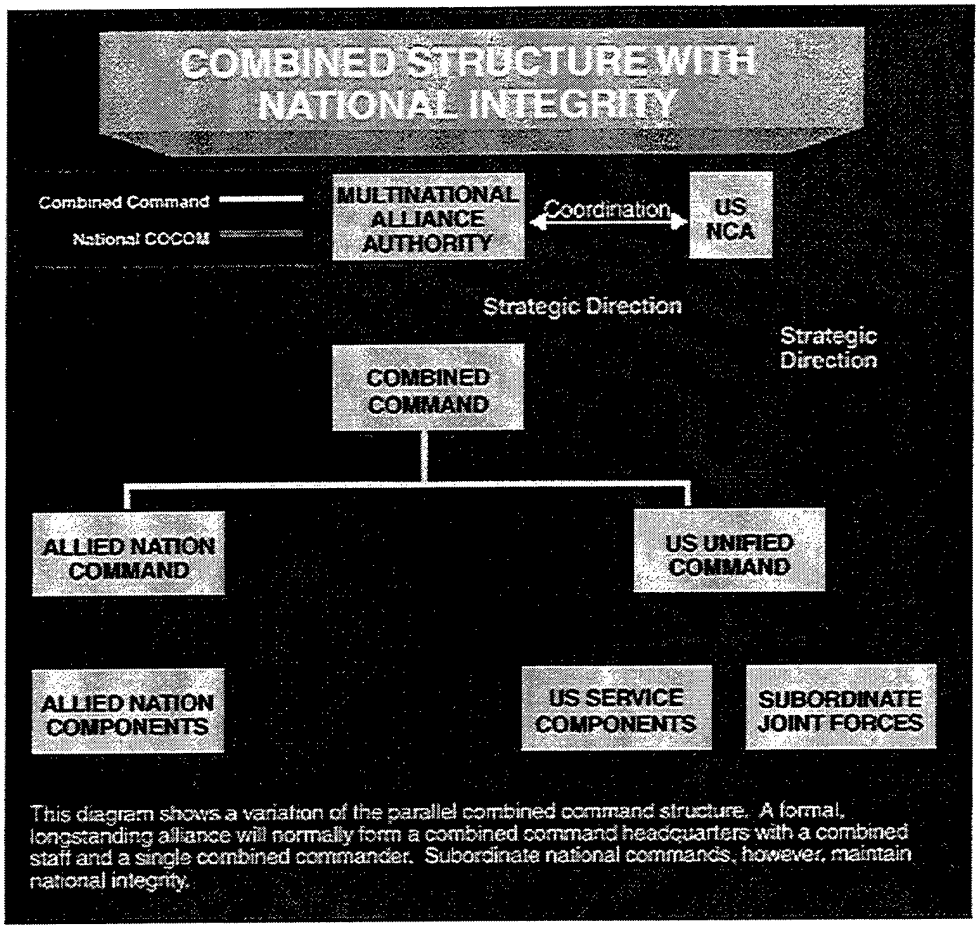


Figure 1.1. Example of a Parallel Command Structure with National Integrity. From Ref. [4]

b. Lead Nation Structure

The lead nation command structure is the opposite of the parallel command structure. In this command structure all coalition members subordinate their forces to a single partner, usually the host nation or nation with majority investment of forces, equipment and expertise. The lead nation's headquarters is typically augmented

with staff representatives from the participating coalition members for two reasons; 1) Staff representation eliminates the perception that the lead nation's actions are preferential to its own interests; and 2) Provides the lead nation with a pool of knowledge from which to draw expertise on the capabilities of the respective coalition members. The resulting structure facilitates the planning process. [Ref. 3 p. II-12]

c. Combination

When coalitions are composed of nations that for political reasons cannot work together in a hierarchical organization, and the use of a parallel structure is not desired, a combination of the two structures is an effective compromise. The command structure consists of two or more nations serving as controlling elements for a mix of international forces. This force structure was in place during Operation Desert Storm and is shown in figure 1.2. [Ref. 3 p. II-12]

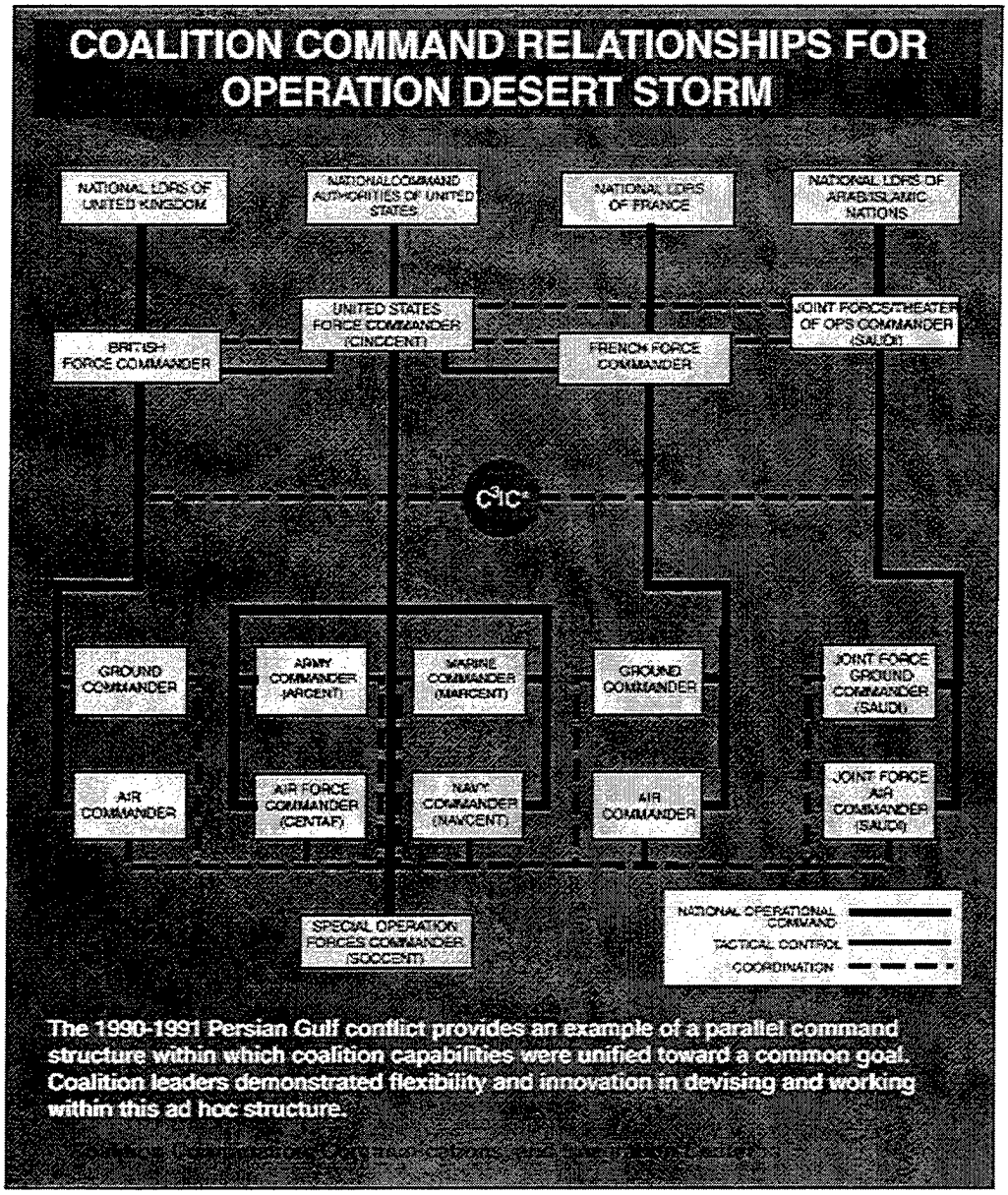


Figure 1.2. Example of a combined parallel and lead nation command structure. From Ref. [4]

Notice the tactical control line linking the British and French Force Commanders to the U.S. Force Commander; this indicates that both of those Force Commanders reported to the U.S. Force Commander. The Joint Forces/Theater of Operations Commander (Saudi) has no tactical control line to the U.S. Commander indicating that although there was

force coordination, his force operated independently of the U.S.-lead nations. This was a necessary political concession to maintain stability and cohesion within the coalition.

2. Command and Control Functions

Command and control functions change very little as a result of the command environment. For instance, a liaison structure is as common in a Joint Task Force as in a Coalition Task Force. However, the need for a coordination center is unique to coalition warfare. Command and control functions are defined in Joint Pub 1-02.

> Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. [Ref. 2]

Common to all the command modes is the existence of a liaison structure. Doctrine, tactics, training, planning and execution require strong and effective liaison along vertical (echelon) and horizontal (peer) command lines. Establishing liaison efforts early promotes clarity of mission and tactics, eases transfer of vital information, cultivates mutual trust, and develops an increased level of teamwork. Early liaison helps smooth friction and lifts the fog of war caused by interoperability problems encountered in communication systems, doctrine and operating procedures. [Ref. 3 p. II-13]

Creating a coordination center is another means of controlling coalition efforts, especially in the case of a parallel command structure. The coordination center is a hub for liaison activity across all boundaries of the coalition environment. It is a place for Non-Government Organizations (NGOs) and Private Volunteer Organizations (PVOs) to conduct civil-military operation planning with their uniformed counterparts, and a

controlled site for military leaders and public affairs officers to brief the news media. Establishing a center for coordination activity enhances stability and interaction.

3. Levels of Command and Control

Command and control structures are segregated into three distinct levels: strategic, operational, and tactical. Each level is designed to focus on a specific layer of military planning and execution. Technologic advances in weaponry and information systems however, blur the lines across functional boundaries. Interconnecting systems make it possible for strategic and operational commanders to evaluate tactical maneuvers and attacks in near real time. As a result the speed of command - the cycle of observation, orientation, decision and action - has increased significantly.

a. Strategic Command and Control

Coalition goals, objectives, policies, and protocol are formed at the strategic level. Control functions employed are secure message, voice and teleconferencing, national intelligence, surveillance and reconnaissance (ISR) sensors, and Indications and Warning (I & W) Systems form participating nation. The level of automated information sharing among all coalition members is very limited at this level due to the classification attributed to data produced by each nation's sensors. There are efforts underway to create a permanent information-sharing infrastructure for strategic planning between Great Britain, Germany, France, Australia, Canada and the United States.

b. Operational Command and Control

Coalition Task Force campaign planning, mission directives, force employment, and resource allocation are decided at this level of command and control. The control functions used are integrated command and control systems for air, land and sea; satellite communication systems; national information systems and coalition wide area networks. Automated information sharing among coalition members is often restricted to a common denominator of data releasable to all coalition forces. This could present a problem when information of a more sensitive nature is required to accomplish a time critical missions. Coalition forces are assigned according to their capabilities. While some forces may need only unclassified or coalition releasable information to fulfill their missions, other coalition forces may need higher sensitivity information, such as targeting or raw sensor information, for example, to fulfill an aircraft strike mission. This information may be releasable to the nation performing the mission under other circumstances, but, because information is flowing within the coalition network, only that information releasable to all coalition members is allowed on the network. Thus another mechanism is required for member-specific information

c. Tactical Command and Control

Implementation and execution of operational plans are carried out at this level. Tactical command and control functions involve the transmission of raw sensor data through use of voice, data, and sensor-equipped weapons systems. Communication must be rapid and precise. Information Sharing on this level presents difficulties because of weapons and sensor incompatibility, lack of information sanitization mechanisms to

filter non-releasable data, and the speed at which these communication must travel (filters may create unacceptable transmission delays or strip away essential data).

D. MISSION OF A COALITION

As stated previously, coalitions are formed to accomplish specific objectives. Those objectives can be accomplished in two ways, wage war or conduct military operations other than war (MOOTW). For the purpose of this discussion war can be declared or undeclared. The command and control structure and function decisions are dependent upon the means by which the coalition intends to obtain its objective. In both cases the topology of the region and remaining infrastructure will factor into structural and functional decisions.

1. War

The Persian Gulf War is a good example of how wars will be fought in the future. The command mode is most likely to follow the lead nation structure. Operational command and control function will be established at a regional headquarters removed from any immediate combat threat, the level of coalition coordination and collaboration will be high. Any commitment of ground forces will be preceded by heavy air bombardment. Resulting damage to the enemy's infrastructure is likely to make it difficult to establish long-haul data networks when ground forces land and begin to establish friendly command and control systems.

2. Military Operations Other Than War

Military Operations Other Than War (MOOTW) has characterized U.S. military operations over the past decade and is likely to continue for the foreseeable future.

MOOTW can be separated into three specific missions: peacekeeping, humanitarian and disaster relief. Any of the above mentioned command structures could be employed during these missions, with parallel being the least preferred. As with wartime operations, destruction to national infrastructure will create problems for establishing local command and control systems. In contrast to war, the need to establish a coordination center in MOOTW is greater because the command structure is more fluid and the coalition less cohesive. Centralized communications creates stronger control functions and supports unity of effort.

E. CHALLENGES IN THE COALITION ENVIRONMENT

The coalition environment is a challenge to work in. As mentioned previously coalitions are dynamic, today's coalition will not respond to tomorrow's crisis. This ad hoc nature makes standardizing doctrine, policy, or operating procedures difficult. As a result the most burdensome challenge facing coalitions is interoperability. This encompasses a whole spectrum of incompatibility issues - doctrine, policy, tactics, language, automated weapons and information systems... the list goes on. Complicating these issues are political sensitivity matters such as those that preclude one nation from working or sharing information directly with another nation or sensitive material handling and releasibility concerns.

Lack of interoperability permeates all levels of command and control. It slows the speed of command and detracts from building unity of effort and purpose. Working outside a common operating environment can lead to misunderstanding of missions, missed opportunity for decisive military action, or blue on blue engagement. Technical solutions such as procuring only those systems that are compatible with allies and

partners for peace members are only part of the answer. The goal of producing a common operating environment lies in coupling technical solutions with policy and doctrine standardization. Therein lies the crux of the interoperability problem: the ad hoc nature of coalition formation precludes policy and doctrine standardization.

F. SUMMARY

Coalitions are ad hoc in nature, formed as a multinational response to a common threat. Once the threat has been eliminated, the coalition dissolves. International politics drive the composition of coalitions. As a result, a coalition is dynamic; no two coalitions are the same. Combined Task Force organization differs with each instance of a coalition and is a reflection of political relations, the mission, and the threat. The function of command and control is meant to lift the fog of war and smooth the frictions and chaos of forming coalitions. However, despite advances in information technology, interoperability problems permeate all levels of military planning and serve to slow the speed of command. Technical solutions to interoperability are only viable if they are coupled with doctrinal and policy changes acceptable to all coalition members.

The next chapter defines a particularly difficult interoperability problem, which once understood and addressed, could ease the difficulties of information sharing and collaboration. That problem is the security of coalition wide area networks.

THIS PAGE INTENTIONALLY LEFT BLANK

III. NETWORK SECURITY REQUIREMENTS

A. BACKGROUND

Whether stand-alone or networked, computer systems share common security requirements. These requirements are based on the security goals of ensured integrity, confidentiality and availability. Security goals are established to counter specific threats to the system. These threats include unauthorized access to the system or system resources, unauthorized modification of files, system attack, and denial of service.

Networked computer systems present additional vulnerabilities to achieving security goals. Communication links that connect individual systems together are susceptible to attack, tapping or disruption. Sharing information across classification boundaries may result in data confidentiality violations. Configuration management of hardware and software in a widespread network is often difficult to control. If the network is linked to an Internet service, the problem of remote access by untrustworthy computing systems is introduced. Widespread-networked systems can attract anonymous user problems associated with unidentified users. A Coalition Wide Area Network (CWAN) manifests all these vulnerabilities and is one of the most challenging networks to secure.

This chapter will define the security goals of computing systems with respect to the coalition environment and articulate the threats that jeopardize attainment of these goals. While some solutions to these computer security threats will be addressed, a more detailed discussion will occur in a subsequent chapter. The objective of this chapter is to introduce fundamental aspects of network security.

B. NETWORK SECURITY THREATS

A network is a collection of interconnected computer and communication transmission mechanisms that provide data communication services. Networks can be limited to a local area, distributed within a metropolitan or wide area, and dispersed globally such as the World Wide Web. Within a network security goals are established to counter threats or vulnerabilities to the operation of the network. Some of the more common threats are discussed below.

1. Traffic Flow Analysis

This subtle threat can cause severe damage to the success of military operations. This is true because information can be inferred by monitoring the quantity and /or types of traffic flows across a network. For example, if an adversary is monitoring the electromagnetic transmissions emanating from the network and notices a significant increase in these emanations followed later by an offensive maneuver, he may anticipate another maneuver should he detect increased emanations in the future. The frequency of traffic may provide indications and warnings to an adversary that something is about to happen, especially if the information flow has increased between specific geographic locations within the network. This may indicate where the next maneuver is likely to take place or which unit will participate. In this instance the element of surprise is lost.

2. Denial of Service

Preventing access to network services through theft or disruption is a denial of service. Disruptions to information flow con occur as a result of flooding the network with irrelevant traffic, delaying the flow of time-critical traffic, blocking information

from flowing to specific addresses or creating a message replay loop. Denial of service can be the result of malicious or benign action. A malicious action might involve deliberate intrusion into network resources to cause a buffer overflow or block an Internet protocol address. Benign actions are often the result of poor user training, lack of management education or understanding, and weak or no security policy enforcement.

3. Spoofing

Spoofing means to fool a system or internal system process into allowing access or privilege by masquerading as an authorized user or process. Spoofing can be achieved by compromising or stealing user identifications and passwords or by modification of internet protocol source addresses.

4. Malicious Software

Malicious software can be an application or other code that is specifically designed to subvert an information system. This malicious software can be embedded into legitimate applications or documents that perform as designed but also infect the system with the hidden code. Such malicious software is known as Trojan Horses. Viruses and worms are types of Trojan Horses which can spread quickly from system to system either through the user unwittingly passing it on to others, as with the virus, or through the self-replication program within the malicious code that e-mails itself to others, in the victims e-mail list, as with the worm.

Other malicious software can be embedded into the system during programming. Trap doors, for example, are artifices, usually located in the operating system, that when triggered permit clandestine control of the entire system.

5. Covert Channels

When system mechanisms are used in an unanticipated way, the possibility for information leakage that violates system security policy is present. Effects and exceptions from the use of system mechanisms can be exploited to move information from one confinement domain to another in violation of mandatory policy. Covert channels are exploited by Trojan Horses.

C. PROTECTING THE SYSTEM

Security mechanisms are created in a system to make certain the system performs as designed despite inexperienced user mistakes or direct attempts to subvert it. Strong security mechanisms can prevent unauthorized access to the system and its resources. Four methods of protection will be discussed; they are system access controls, data access controls, system and security administration and system design.

1. System Access Controls

Protection of a system starts with user identification and authentication (I & A). These mechanisms are used to verify that individuals accessing the system are authorized users. There are three ways of identifying a user to the system:

- Something the user knows such as a password
- Something the user has such as a card, token or key
- Something the user is, typically a physiological trait such as fingerprint or retina pattern [Ref. 5]

Often more than one of these identification methods is used. For example, to access a bank's Automated Teller Machine (ATM), the user must present a card and input a personal identification number.

While identification and authentication of the user to the system is a positive step in system security, the user must be assured that he is communicating with the real system and not a malicious code designed to steal authentication symbols. To do this a valid link is invoked between the machine and the system called a trusted path. This gives the user assurance that he is authenticating himself to the actual operating system.

2. Data Access Controls

Data access controls monitor who and how data can be accessed. There are two methods for providing this control: Discretionary Access Control (DAC) and Mandatory Access Control (MAC). Both can be used to enforce integrity and confidentiality rules.

a. Discretionary Access Control

Discretionary Access Control (DAC) policies are access controls established by the data owner and used to enforce modification integrity. Access controls can be set in place by first defining individuals (subjects) as owners or users of pieces of data or files (objects). The owner of a file grants permissions to view and/or modify that file to select users. The permissions are read, write, execute, delete, change permissions and revoke permissions. The owner of the data can retain the ability to grant and revoke permissions. Subjects are restricted to performing only those permission functions on objects for which they've been granted access. The operating system maintains a list of permissions granted for each user called an access control list. This list is not directly accessible to system users but is interpretively accessed.

Well-intentioned users and malicious attacks can subvert discretionary

access controls. For example, user A may copy a piece of data, for various non-malicious reasons, and send it to user B who did not have access. User B now has access to the data and can copy the data to other users perpetuating the loss of confidentiality. An example of a malicious attack is the introduction of a Trojan Horse into a system. While the program is executing valid functions it may also be copying files from authorized users into the directory of the malicious user.

b. Mandatory Access Controls

Mandatory Access Controls (MAC) policies were developed to take the access control decision out of the hands of the individual and centralize it within the operating system. To implement this, individuals' clearance levels and information sensitivity labels such as Unclassified, Confidential, Secret, Top Secret and Sensitive Compartmented Information (SCI) must be established. The ability of an individual to access information is dependent upon a comparison of individual session levels and information sensitivity labels. Comparisons are performed using a dominance operator similar to the mathematical operations greater than or equal to symbol "$\geq$". For example, using the classification level described above:

SCI $\geq$ Top Secret
SCI $\geq$ Secret
SCI $\geq$ Confidential
SCI $\geq$ Unclassified
Top Secret $\geq$ Secret
Etc. [Ref. 6]

To access a system the user must initiate a session level at or below the information sensitivity level for which he has been granted security clearance.

(1) Security Models. Two security models have been designed to enforce confidentiality and integrity security policies. The Bell and La Padula Security Model [Ref. 7] protects confidentiality while the Biba Integrity Model [Ref. 8] protects integrity. Bell and La Padula introduced two rules that when used together prevent unauthorized disclosure. The Simple Security Property does not allow an individual to read information at a higher classification level but will allow access to lower levels. Therefore, a user cleared for access to Secret data cannot read Top Secret data but can read Confidential data. In this case read down is allowed while read up is not allowed. The Star Property (*-Property), on the other hand, prevents information from being written from a higher to a lower access level. For instance Top Secret data cannot be copied down to Secret data. This prevents unintentional human error and malicious code from resulting in unauthorized disclosure. Figure 3.1 shows an information flow diagram using the BLP Model.

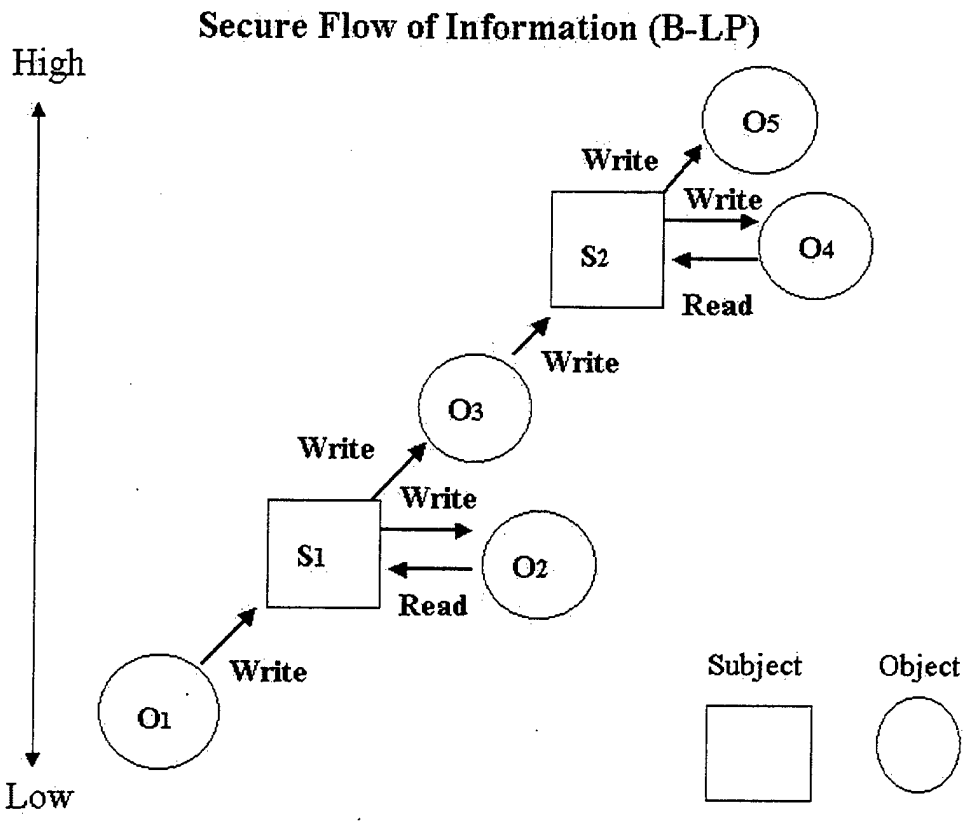


Figure 3.1. Illustration of Bell and La Padula Security Model. From Ref. [6 Sec3 p.8]

In the Biba Integrity Model, integrity levels, such as high, medium and low, are applied to both system processes and information. In this model, Biba's two properties, similar to those of the BLP model, enforce integrity. The Simple Integrity Property restricts write access, while the *-Property restricts read access. These properties are founded on a hierarchy of subject and object classification levels. For instance, if user A wishes to add a lower releasibility paragraph to a higher releasibility document, the Simple Integrity Property prevents a write up of the lower integrity data to higher integrity data. The *-Property prevents a subject at a higher integrity level from reading information at a lower integrity level. Figure 3.2 illustrates the Biba Model.

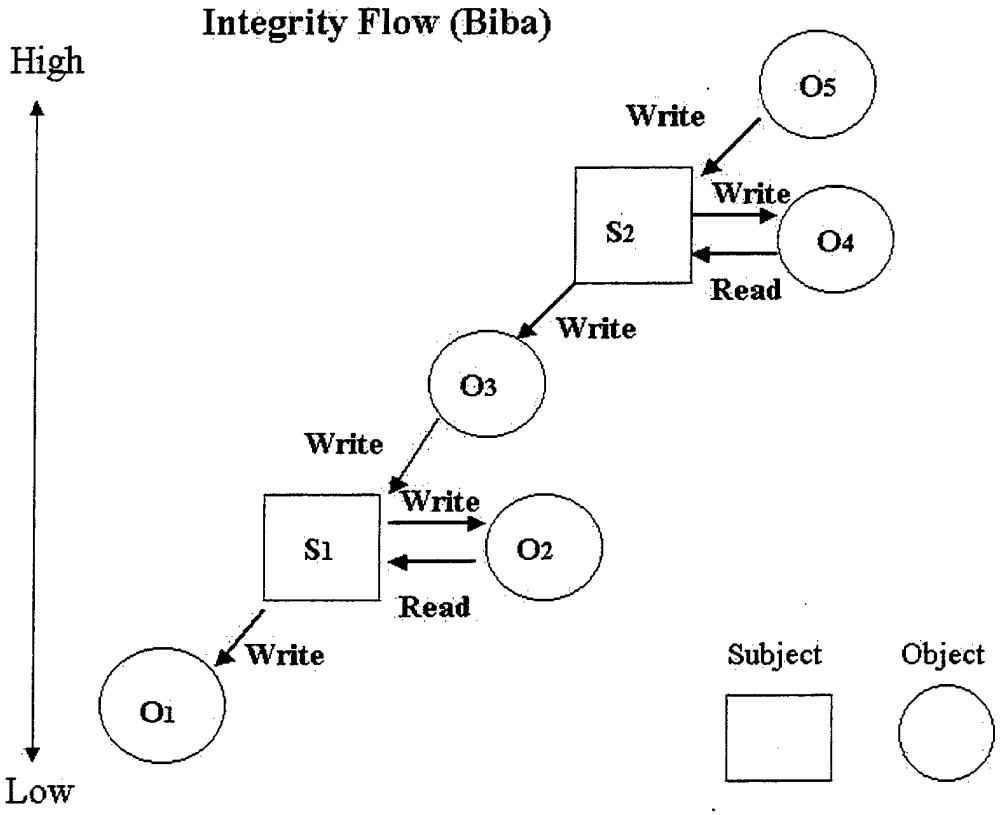


Figure 3.2. Illustration of Biba Integrity Model. From Ref. [6 Sec 3 p. 18]

A computer system enforcing the BLP security model restricts the untrusted user to one information sensitivity level. For example, a user may initiate a session level at the Secret sensitivity level if he is cleared to view Secret data. If that same individual desires to write Confidential data, he must close the Secret session and initiate a new session at the Confidential level. He may not initiate a session at the Top Secret information sensitivity level because he is not cleared to view Top Secret data.

There are times, however, when the integrity of the information supercedes or is as important as maintaining confidentiality. The integrity of positional data, for instance, is of extreme importance. Using the Biba Integrity Model a lower integrity user cannot write targeting information to a higher integrity document or program.

3. Nonrepudiation

Cryptography complements and strengthens access control host-based mechanisms. In a distributed system there is a need to protect against the sender of a message later denying the transmission of that message. This is called nonrepudiation and is implemented by a combination of symmetric and asymmetric key ciphers where the latter is known as Public key cryptology. Public Key protocols use two keys, one private and held securely, the other public and distributed to everyone. Messages encrypted with a user's private key can only be decrypted using the user's public key. Hence, there is no refuting the authenticity of a transmission (provided the private key remains securely held).

A digital signature is an encryption method used to ensure information has not been modified en route to its final destination and has maintained its nonrepudiation characteristics. Similar to a handwritten signature, a digital signature must be verifiable and must not be forgeable. Digital signatures can be achieved using a public key scheme and a hashing algorithm. A hash is introduced prior to message transmission to provide the message with a fixed sized thumbprint. This thumbprint is known as a message digest and provides a manipulation detection code for the message. This code provides a cryptographic checksum, comparable to the checksum digit at the end of a number sequence in a military AUTODIN message. Once the packet is received a second thumbprint can be computed by the receiver and compared to the transmitted thumbprint. If they match, the message has not been altered. Just as the number checksum ensures that a number sequence was reproduced correctly in a message, the manipulation detection code ensures that the hash of the message is equivalent to the original message.

To prevent forgery and maintain integrity, the encrypting algorithms must be easy to compute but mathematically infeasible to reverse within a given period of time without the correct cipher key. Ref. [6 Sec 7 p. 42]

4. Availability

Availability has many contextual meanings. It can refer to either the system or data. For simplicity, availability is defined as the fair allocation of system resources, consistent with access control policies, in a usable format, and at a capacity to meet quality of service needs. A network must be simultaneously accessible and able to manage packet collisions with no noticeable disruption of service. Some threats to availability include denial of service attacks, misconfigured hardware or firmware and loss of power. Availability can be assured through robust physical security policies, strict configuration management, correct configuration of routers, switches, firewalls, and intrusion detection systems, and most importantly, vigilant attention to audit logs.

5. System and Security Administration

Establishing and adhering to system and security administration procedures is fundamental to pursuing network security goals. System administrator responsibilities, such as performing back ups, ensuring proper hardware and software configuration and performing consistent audit log reviews must be clearly defined and understood. Training new users prior to activating their accounts can pay dividends in avoiding system downtime due to inexperienced users and security violations. Security administration also involves conducting periodic assessments of the threats the system may face as a result of added hardware, software, or expanding network services provided.

6. System Design

Secure systems begin with a secure design. Historically the Trusted Computer System Evaluation Criteria (TCSEC), known as the Orange book, was a tool to help design engineers and information security specialists understand the requirements necessary to provide the level of security desired for their system. The TCSEC permitted certification of computer systems based on the extent to which that system met four system security requirements:

- Security Policy – such as DAC and MAC
- Accountability – such as I & A, auditing, and trusted path
- Assurance – such as system architecture, system integrity and
- trusted recovery
- Documentation – such as test and design documentation
- Security policies and Accountability have already been addressed. Assurance and Documentation will be addressed below.

The TCSEC divided system assurance levels into four divisions ranging from A to D, with D being the lowest level of assurance. These divisions were subdivided numerically with 1 as the lowest and 3 as the highest level of assurance within each division. For example, a system rated C1 satisfied a lower set of assurance criteria than a higher assurance rated system such as C2.

a. Assurance

Assurance, with regard to computer systems, refers to the level of trust or confidence that a system's security policies are enforced. Some software system architecture security techniques for achieving assurance are:

- Layering – a structuring software into loop-free layers that only call down

- Modularity – structuring software into small, single purpose understandable code units
- Data Hiding – structuring data so that the details of how modules manage memory is hidden in encapsulated, well defined interfaces
- Principle of least privilege – processes or programs are given only enough privilege to perform their specific task [Ref. 6 Sec 4 p. 22].

These software architectures are designed to be small enough to be easily tested and verified to be logically correct. Figure 3.4 illustrates layering and modularity.

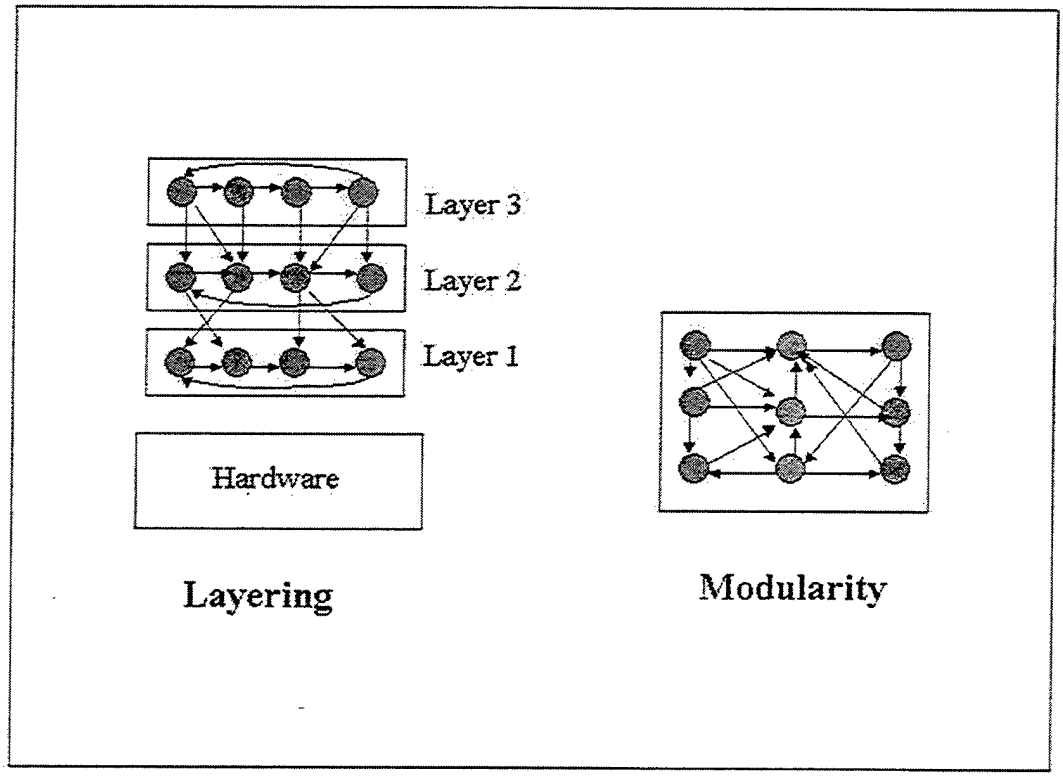


Figure 3.3 Illustration of software Layering and Modularity

Hardware assurance techniques include designing a security kernel, and protecting memory and addressing by dividing memory into separate pieces or segments.

b. Documentation

Documentation is a prerequisite to TCSEC certification on all C1 and above systems. Detailed documentation of system design as well as test plans and results must be provided. A Security Features User's Guide summarizing the system's protection mechanisms and Trusted Facility Manual detailing proper secure facility administration are also required.

Today the "Common Criteria" [Ref. 9] framework serves a similar purpose, providing guidance for system developers, standards and requirements specification for systems, and a form of quality control for customers.

D. NETWORK SECURITY CHALLENGES IN A COALITION

The coalition environment presents unique challenges to network security. Coalition networks incorporate geographically dispersed nodes connected by a variety of communication links to a common backbone that terminates in a Communications Department at the Task Force Headquarters. The complexity of the system and degree of information sharing required in a coalition conspire to magnify the vulnerabilities associated with meeting network security goals.

1. Complexity

Complexity in a network can refer to the architectural infrastructure, or the intricacies of hardware and software relationships. Both contribute to the difficulties of creating a coalition network. While it is not the intent of this research to focus on network architecture, communication links, and system interfaces, a meaningful discussion of security requirements would be remiss to dismiss the subject.

Architectural infrastructure refers to the individual computer nodes, server banks, hubs, switches, routers, and communication links that interconnect to create a local, metropolitan or wide area network. In a coalition, the infrastructure is provided by several nations. Technology gaps or differences between nations make integrating systems difficult. To accommodate additional requirements, system interfaces are modified to behave in a manner outside original parameters. These "work arounds" enable connectivity but may trigger security vulnerabilities. Coalition network infrastructures often span large geographic areas that have been devastated by aerial bombing. Consequently, local landlines are damaged and unusable. In mountainous regions, communications by line of sight may not be appropriate. Therefore wireless communication links, such as microwave or satellite, are introduced to establish connectivity. This opens more avenues for potential loss or unauthorized disclosure of information.

Configuration management, the process of controlling changes to network hardware and software, is difficult to monitor in a wide, geographically separated network. Unauthorized installations of peripheral devices or software can introduce security vulnerabilities. Internet access invites remote system access by possible malicious users leaving the system open to many points of attack.

2. Sharing Information

In Joint Vision (JV) 2020, the Chairman of the Joint Chiefs of Staff clearly states that future military success is directly linked to obtaining Information Superiority. A critical element of Information Superiority is the seamless sharing of information across all echelons of battlefield command and control. Sharing sensitive or classified

information across multinational boundaries is one of the greatest challenges to coalition interoperability. There are several problems associated with network interoperability that are rooted in both technologic and policy limitations.

a. Strict Disclosure Policy

Each nation in a coalition must adhere to its national disclosure policies. These policies identify what type of information is releasable to which country under what circumstances. Modifications to these policies are not trivial and take time to be approved. In some cases national law may preclude one nation from sharing information with another nation, thereby making modification of that policy even harder.

Sharing information among nations in an alliance is much simpler. NATO allies, for instance, have been sharing information for decades based on strict disclosure policies agreed to by all member nations. However, even within NATO, procedures for disclosure of information outside the alliance are very burdensome and require the approval of all nineteen nations.

Coalitions, on the other hand, are formed rapidly with no plan for how and what type of information will be shared. In fact, the information to be shared and with whom is dependent on the mission (peacekeeping, humanitarian, war) and composition of the coalition. Thus information-sharing decisions are made "on the fly". As a result there may be pockets of information available that are not exploited because the right people do not know of its existence or those who control the information do not know to whom the information is releasable or how to get the information to the right authorities for dissemination. [Ref. 10]

b. Information Not Uniformly Labeled

Labeling information properly is contingent upon identifying the sensitivity level of the information. The task is much easier in an alliance than in coalitions because there has been time to come to consensus on standardization of sensitivity level definitions. Alliances and individual nations have their own set of criteria by which information is judged to be critical to the interests of the nation or alliance. For example, in the United States, unauthorized disclosure of information that would result in grave consequences to national security is labeled Top Secret, while unauthorized disclosure of Secret information would have serious consequences to national security. Therefore labeling information requires agreement on the damage that would result due to unauthorized disclosure.

Terminology differences also prevent standardization on information labeling. What the United States considers Confidential information may be equivalent to another nations label for Restricted, and U.S. Secret equivalent to Confidential in another nation's terminology. Agreement upon terminology and information sensitivity level labeling takes diplomacy and time. The dynamic nature of coalitions hinders this initial negotiation. If the coalition becomes longstanding, (greater than 6 months), there is adequate time to reach a consensus. Unfortunately, the consensus ends when the coalition dissolves and the process starts again with the next coalition.

c. Filters

Filters are software or hardware placed at boundaries between systems that have differing levels of information access. Filters are intended to act as a barrier

between systems, preventing the higher classification system from disclosing information to a lower system, while simultaneously letting authorized information through. They are sometimes referred to as guards. Each guard is programmed with specific code, based upon rule sets, to pass information fitting certain criteria while rejecting information that does not. The rejected information is routed to a queue for human intervention. Although filters facilitate information sharing, they are limited as to their ability to filter all information. Information fed into filters must be organized into a format that the filter recognizes such as Over the Horizon (OTH) or U.S. Message Text Formats (USMTF). If the format is incorrect, the filter cannot implement its programmed rule sets and rejects the information. At this point the human providing intervention must have access to all information crossing the network to make the determination to override the filter or not. This limitation of the filter precludes the sharing of non-formatted information such as documents and e-mail. In addition, sensitive information can be encoded in messages that can successfully pass the filter's rules. This weakness allows Trojan Horses to move information from High sensitivity to Low sensitivity domains. Filters are also limited in their ability to implement multilevel security operations. Most filters have not been designed to differentiate between data releasable to one nation from that releasable to another, as a result the information coming from a filter is releasable at the highest level of clearance common to all member nations. This hinders the seamless, transparent information sharing espoused in JV 2020. Alternatively, several separated filters could be used to pass releasable information to individual nations. However, this solution may be too costly in terms of equipment and man-hours.

d. Bandwidth

Differences in technical capabilities among coalition members severely limit the bandwidth capacity along the network. Disparity between processing units on a network or communication link limitations result in slowing the flow of information. Since most networks do not recognize data precedence, data requiring timely delivery may be held up awaiting availability on the network. These are called Quality of Service (QoS) issues. Currently to avoid delays on tactical networks, standard operating procedures are implemented to limit the unnecessary transmission of high bandwidth products such as PowerPoint presentations. However, some high bandwidth products, such as imagery, are essential to achieving information superiority.

e. Language and Cultural Barriers

Finally, language and cultural barriers negatively impact coalition interoperability. This affects social as well as network relations. While liaison officers and interpreters ease the problem, the cultural meaning to words does not always translate well, consequently there is room for misunderstanding and friction.

E. SUMMARY

This chapter has addressed the security concerns and difficulties related to network computing in a coalition environment. The security goals of integrity, confidentiality and availability by themselves are a challenge to achieve on a homogeneous network. The complexity, heterogeneity, and information sharing concerns of a coalition network makes achieving these security goals daunting. Standardization of policy, doctrine and terminology would help bridge the cultural gap and facilitate

interoperability. The next chapter will identify the network security requirements associated with coalition networks.

IV. COALITION NETWORK SECURITY REQUIREMENTS

A. INTRODUCTION

The magnitude or modern warfare, in regards to the ability to project power globally and the speed with which decisions can be made and acted upon, requires robust information system architectures to synchronize the efforts of warfighters. The diversity of a coalition makes synchronization especially crucial not only to engage and defeat the enemy but also to ensure the safety of friendly forces. Therefore, a coalition network, regardless of the mission it is supporting, must meet certain capability requirements.

> Basic to the conduct of these operations is the ability to develop and maintain a shared perception of the situation, develop coherent plans that leverage the available resources, and execute them. This requires a level of information exchange, systems that can understand one another, a coalition-based planning process where all may participate, a common concept of operations, and a set of compatible procedures to carry out operations. [Ref. 11 p. 226]

This broad requirements statement identifies three technical capabilities: information exchange, systems interoperability and collaboration; and two policy driven requirements, a concept of operations and standard operating procedures. These capabilities and requirements will be addressed in terms of the security-related mechanisms and policies required to implement them.

B. INFORMATION EXCHANGE REQUIREMENTS

Information exchange in a coalition entails data flows between high and low sensitivity networks. In the past this data flow has been facilitated by air gapping the data between two physically disconnected systems. This can add a degree of latency that is unacceptable for current command and control systems and weapons capabilities.

The information exchange requirement is to provide a secure means for information to pass between high and low sensitivity systems among users appropriately cleared and authorized for the level of information they are accessing. Multilevel security (MLS) provides the capability to simultaneously store, process and share information of varying sensitivity and information levels with users who have a variety of clearance levels, authorizations and need to know. [Ref. 12]

Security policies for data releasibility and information handling must be established before MLS can be implemented. When that policy is encoded for system use, a level of flexibility must be built in to allow for modification due to changes in the composition of the coalition. Flexibility in the encoded policy will enable reuse when new coalitions are formed.

1. Multilevel Security

Multilevel security capabilities are found in TCSEC Division B and A systems. These systems implement security labeling mechanisms that enforce MAC policies. Class B1 systems and below are classified as low assurance systems because they do not require the same degree of testing and proof of correctness required of class B2 through class A1, the high assurance systems.

There are a variety of MLS or Multi-security level (MSL) technologies that can be implemented as a partial solution to the coalition information exchange problem. These component technologies include hosts, workstations, guards, and database management systems. Integrated together, these technologies can form MLS architecture. This architecture, however, need not be composed solely of trusted systems.

Multilevel security capabilities can be integrated with single level systems to separate and protect data of different sensitivity levels where required.

a. Label Requirements

The TCSEC requires sensitivity and label integrity be associated with each subject and object within a system. Label sensitivity refers to the classification level assigned to information, while label integrity ensures exported labels mirror internal labels, meaning unauthorized persons cannot modify them. Exportation of labeled information requires that input/output devices be properly labeled single-level or multilevel and tested to verify correct implementation. A trusted system is required to label data output with a human readable marking that conforms to established security policy. In addition the system is required to notify the user of each change in session level as the system is used. For example, if the user begins work at a confidential sensitivity level, then decides to initiate a secret sensitivity level session the terminal will alert the user as to the change in sensitivity level. [Ref. 6 Sec 6 p. 38] Some systems allow simultaneous multiple sensitivity level sessions. In this case a user can initiate multiple sensitivity sessions, much the same as multitasking in a Windows Operating System environment, and work on documents at various sensitivity levels. The system indicates the sensitivity level of the active window.

b. Multilevel Security Technologies

Several MLS technologies can be used to achieve coalition information exchange requirements. A combination of technologies listed below can be integrated with legacy or single level systems to form a MLS federated system.

- MLS Hosts – a term that describes the basic components of computing systems used for data processing and transfer services such as a workstation, web server, file server, mail server and print server. [Ref. 12 p. 6-7]
- MLS Guards – these are one-way (low-to-high or high-to-low) or bi-directional filters that provide the connectivity required to bridge across the security boundaries of systems operating at different security levels. Low-to-high filters might be used to prevent the transfer of malicious code or attempts to deny service by flooding the network. High-to-low filters verify the security level of data headed to the low system by performing "dirty word" checks, through human review, or by checking to ensure that data have specific sensitivity labels. Data that successfully complete the checking process are downgraded and passed to the low side. [Ref. 12 p. 7]
- MLS Workstations – a workstation that performs its own processing and storage and can separate and protect data of different security levels. A compartmented mode workstation provides multilevel, multiwindowing capabilities that allow users to access windows of different security levels simultaneously and transfer data between them. This workstation meets specific Defense Intelligence Agency requirements for multilevel and compartmented mode operations. [Ref. 12 p. 7]
- MLS Data Base Management Systems – these systems serve as the cornerstone for many MLS applications. A MLS DBMS uses security mechanisms, such as a comparison of sensitivity labels to user clearance and privilege levels, to grant users modes of access to information and to allow modification by authorized users. Similar security mechanisms are used to control user queries. [Ref. 12 p. 8]

Coalition networks can use a combination of the above MLS technologies to provide a secure interconnected network environment provided a strong yet flexible security policy has been defined and system interoperability is established, tested, certified and accredited by proper authority prior to implementation. Unfortunately the lead-time required to achieve this level of secure network environment impedes progress toward a truly interoperable, seamless coalition network.

C. SYSTEMS THAT CAN UNDERSTAND EACH OTHER

System interoperability requires more than compatible hardware and operating systems. Joint Pub 1-02 defines interoperability as:

> "The ability of systems, units or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together." [Ref. 2]

In a coalition environment, this means that the systems must accept, process and distribute information between each other while enforcing information security policies – a very tall order for a network comprised of systems ranging from legacy 386 processors to Pentium III processors or XTS 300 platforms.

Providing the physical connectivity between disparate systems in a coalition is technically feasible and has been accomplished to some degree during operations in Bosnia and Kosovo; managing the connectivity, however, has become the Achilles heel of coalition interoperability. [Ref. 10] Current interoperability problems are rooted in formatting mismatches and an inability to enforce security policy across network connections.

1. Formatting

Meaningful communication between computers is predicated upon the computers ability to process the information it is sent. Each nation in a coalition brings with it systems that are designed to accept specific data processing formats. When those formats are common with those of other member nations, interoperability is not difficult to achieve. The question to be answered is how to ensure that each nation brings systems that will accept and process common format.

Some nations look to foreign military sales (FMS) programs to help alleviate the problem, however, FMS may serve to exacerbate the problem. The United States, for instance, maintains a blistering technology replacement pace; key information systems are upgraded every 18 to 24 months. Although the U.S. offers many of its systems in foreign military sales (FMS) programs, those systems are not the most recent software version being used by U.S. forces. In fact, depending on the purchasing nation, the

system may be several versions behind those used by the U.S. and other nations. Sometimes the software upgrades may change the internal processing enough to render the information format commonly used in past versions of the system useless. Consequently, if coalition partners purchase information systems from the U.S., they are destined to perpetually lag in technologic capabilities.

Many nations prefer to use systems acquired through their national acquisition and development process in order to tailor them to their own warfighting needs. While this is certainly logical and acceptable, specificity of systems may result in specificity in data formats. This can lead to information formatting incompatibility when those systems are deployed and integrated in support of coalition efforts. One solution to this problem is to come to consensus on the type of information systems and formats to be used for coalition operations. To this end, a Combined Communication Electronics Board (CCEB) was stood up consisting of representatives from several nations to establish standards for communications and information systems. While conforming to standards will facilitate coalition interoperability, many nations may fear standardization because today's friend may be tomorrow's foe and standardization does away with any unique national information system capabilities that might be perceived to provide individuality or protection. A possible resolution to this issue is to develop dual mode systems, a system that can shift easily from a standardized coalition mode to a unique national mode through a configuration process or the introduction of hardware/software changes. Of course this may be difficult to implement in the lower layers (i.e. network, data link and physical network hardware) of the network stack. In addition, it may introduce vulnerabilities in the systems. For example, an adversary might be able to

cause the wrong node to be switched on thereby gaining unauthorized access to the other network. Security vulnerability and interoperability trade-offs must be considered through risk analysis before decisions are made.

Another solution may be to develop universal translators that will translate any information processing format into the format required for processing on a specific system. For example, if a system that process only formatted messages is presented with a free form text message, the universal translator will scan the document and translate the relevant information from the received message into the format acceptable for that system. The trade-offs here may be in the form of increased latency, semantic errors, or incorrect translation of coordinates. Vulnerabilities introduced may be the possibility of error loops that could result in denial of service, or the modification of the recognition process to translate the data incorrectly, or buffer overflow attacks resulting in denial of service.

Regardless of the solution pursued, the security needs of a network must be considered early in the requirements phase of system design. In this way, security is built into the architecture as well as the tools used to manage the coalition network.

D. SECURE COLLABORATION

Secure collaboration can be conducted asynchronously by using e-mail or file sharing or synchronously by using teleconferencing or application sharing. Regardless of the temporal factor of sharing information, a crucial enabler for secure collaboration is a strong method of encryption to protect the confidentiality of the information. Encryption requires both sender and receiver to have identical cipher keys. Symmetric key management is extremely difficult in a coalition environment because of stringent

national cryptographic disclosure policy and the number of keys required to enable communications. Public key cryptography, on the other hand is much easier to distribute and manage. Public key infrastructure (PKI) involves the secure issuance, by an approved Certificate Authority, of public and private encryption keys for creating a digital signature. The digital signature provides an added benefit. Because the coalition network is geographically dispersed, strong authentication and nonrepudiation is required to ensure that the entity at the other end of the connection is the authorized user and that messages sent by that user may not be repudiated at a later time.

1. Asynchronous Collaboration

Communicating through electronic mail has become an essential part business in the Information Age. In fact, e-mail can be sent to anyone who possesses a computer, modem, Internet protocol (IP) address and the supporting application software. However, when the information communicated is of a sensitive nature or has sensitive attachments and must traverse a multilevel security system, a guard must be implemented to protect that information. The standard mail guard (SMG) is a U.S. National Security Agency approved system that can be used to control e-mail traffic between high and low classified networks. When e-mail with attachments are sent from high to low classified networks the originator reviews the attachments and places an appropriate sensitivity label on it. The SMG verifies the label and allows the e-mail to pass if it meets network security policies. [Ref.13 p. B-11] This assumes that the high side system correctly implements labeling policies and cannot be subverted by the user. Using a digital signature in conjunction with SMG would provide for information integrity and nonrepudiation.

Utilizing standard formatting and implementing MLS technologies facilitates protected information sharing across a heterogeneous network. In addition, use of a public key infrastructure complements MLS technology through the addition of digital signatures for identification authentication and nonrepudiation.

2. Synchronous Collaboration

Synchronous collaboration such as teleconferencing, or participating in a real time chat forum, with an international variety of coalition members requires information be communicated at a coalition releasable level.

E. SECURITY POLICY

The foundation on which network protection is built is a strong, definitive security policy. While the policy should not detail how to achieve protection, it should clearly and unequivocally state those items that are to be protected. Effective network security is consistent. This means that it is applied at all times, whether it is being stored or traversing the network; and that is applicable to all users, operators, technicians and managers; and not optionally employed.

Security policy is a broad term that can have several meanings. For the purposes of this discussion security policy has three contextual meanings, security policy objective, organizational security policy, and automated security. [Ref. 14]

> the core concern of security policies is controlling resource access and use by individuals according to their authorizations. [Ref. 14 p. 227]

At the heart of a security policy is the security policy objective. It specifically addresses the intent to protect information by preventing unauthorized disclosure, unauthorized modification and unauthorized distribution. [Ref. 14 p. 222] Defining

security policy objectives requires placing value on the information being protected. The value can be couched in terms of the cost of loss or disclosure of the information and in terms of value added to situational awareness or tactical advantage if the information is shared. Therefore quantifying the value of information identifies not only the need for protection, but also the extent to which items should be protected or shared.

Organizational Security Policy (OSP) regulates how security policy objectives will be achieved. It specifies the conditions by which users are granted access rights and the rules governing the exercise of those rights. [Ref. 14 p. 223] Organization security policies can be likened to the rules of a board game, to play the game properly players must understand the goal, their roles and under what circumstances they may traverse the board to win the game. In this way OSPs are an awareness tool. An OSP may include the following:

- Data/Document Labeling and Marking scheme and policy – provides clear guidance on disclosure and information handling policy within the coalition. May be a separate addendum covering specifics for each nation
- Identification and Authentication – the importance of PKI and password policy
- Encryption – guidance for use of digital signatures and cryptology
- Storage and printing restrictions
- Configuration Management – policy guidance concerning adding or removing hardware or software items to network nodes
- Explanation of threats to network operations and what to do if the user thinks their node has been compromised

Automated Security Policy (ASP) is the encoded policy that implement the organizational security policy in the computer system. An ASP is generated through the use of system engineering processes that distinguish the portions organizational security

policies that can be automated from those that cannot and identifies the computing processes that can enforce the automated OSPs. [Ref. 14 p. 224] To summarize:

> an ASP must always be used in the context of an OSP that tells users and system administrators how to use the system in compliance with identified security policy objectives. [Ref. 14 p. 224]

Given the above discussion, security policy objectives of each coalition member nation are set forth in their respective national disclosure policy. These policies should be reviewed and modified as appropriate to generate a coalition security policy objective. Once the security policy objectives are known, a coalition-based organizational security policy can be determined and from this automated security policies can be incorporated into the coalition wide area network.

1. Common Concept of Operations

In the capabilities statement above the speaker referred to a common concept of operations. In this instance, he was referencing a common strategy of campaign execution. However, for the purposes of this paper the term will be borrowed and defined as the concept of coalition wide area network operations. Many times in coalitions operations, networks evolve rather than are planned, as a result few people are prepared to seize upon opportunities to improve the network because there was no vision to guide development or plan for the unexpected. [Ref. 10] Just as a concept of operations provides direction to meet campaign objectives, so too does a network concept of operations provide the framework from which policy is derived. A network concept of operations answers questions about deployment and employment of the network. It addresses contingency plans, forensics, and recovery plans should an attack or non malicious event disrupt network services; describes the release and disclosure policies for

information; defines network protection methods; differentiates between each nations local area network and the coalition wide area network; delineates responsibilities of each nation with regard to administration, maintenance and repair of the common network and their own national local area network; and provides a plan for disassembly and disposition of resources of the network upon dissolution of the coalition.

2. Standard Operating Procedures

Standards are rules or regulations that support policy while procedures are the systematic actions followed to accomplish a task. These rules and regulation are combined with step-by-step actions to form standard operating procedures. Standard operating procedures are an effective, efficient and safe means to implement security policy. If written correctly even a novice user will learn to operate the system with little trouble minimizing the ill effects to the system caused by inexperienced, uninformed users. Standard operating procedures are invaluable to proper coalition network operations. The international diversity of users combined with the variety of network operating experience can result in misunderstandings regarding expectations for network operations leading to service interruptions unless user actions are controlled by a common operating procedure. These procedures also help to bridge the cultural, technical and language gap by putting instructions in writing, leaving little room for implicit interpretation and understanding.

F. SUMMARY

This chapter has identified five security requirements for network operations within a coalition environment. The first and second requirements, to exchange information and achieve interoperability respectively, are satisfied by implementing

multilevel security concepts across both trusted computing base multilevel and non-trusted single level systems that share compatible operating systems and data processing formats. The third requirement, the ability to collaborate, results from implementing cryptologic functions and key management methods, such as those suggested by a public key infrastructure, to achieve confidentiality across a distributed network. A more tenable definition of security policies was provided to give contextual meaning to the term "security policy". Finally, the fourth and fifth requirements, to implement a common concept of operations, and a set of compatible procedures to carry out operations, were broadly defined as the need to produce security policy that incorporated a strategy for network operations and standard operating procedures to overcome cultural, technical and language gaps present in coalition operations.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CURRENT SOLUTIONS

A. INTRODUCTION

Since the end of the Cold War in 1988 the U.S. has been involved in several military operations other than war. Of these operations, only two, Operation Just Cause - the 1989 American intervention in Panama, and operations in Haiti were unilaterally conducted. For over a decade, the U.S., its Allies and Partners for Peace have been struggling to establish command, control, communication, computer and intelligence (C4I) interoperability. While technology has provided the ability to connect networks, it has only recently afforded a degree of security to those connections. This chapter will explore three secure network solutions that are being tested, experimented with and deployed to provide the elusive, seamless connectivity sought in coalition operations. Included in the discussion will be the boards and committees that have championed these technologies and are helping to guide the military into a twenty-first century fighting force.

B. CURRENT SOLUTIONS

Meeting the connectivity and communication goals espoused by Joint Vision 2010, the frustration with mediocre network communications during real world operations, and pressure from the U.S Congress and foreign governments has resulted in a greater research and development push to resolve joint and coalition interoperability problems. The first fruits of this endeavor are being tested in operational experiments and deployed in command ships and regional network operation centers. While there are

several systems being developed this discussion will be limited to three initiatives that either are in testing or have been deployed in the field.

1. Content-Based Information Security

Content-Based Information Security (CBIS) is a joint initiative of the U.S. Joint Forces Command and Space and Naval Warfare (SPAWAR) Systems Center San Diego. It is part of the Department of Defense Advanced Concept Technology Demonstration (ACTD). CBIS is not a fixed system solution, but a "proof of concept" technology that supports protecting information based on its content at the point of origin rather than implementing security mechanisms to protect a network on which various levels of classified information resides or transits. CBIS uses a defense in depth philosophy by encrypting information at the originating workstation and then encrypting it again as it transits the network. The encryption is based on the information content sensitivity and the user clearance level and authorizations. The CBIS solution incorporates familiar information security principles:

- Marking – Labels are bound to the information at its origin, encryption is based on the label bound
- Identification and Authorization – Strong Identification and authorization coupled with biometrics
- Access – Information is shared based on a match between the content label and the user's security attributes

The CBIS components, shown in figure 5.1, consist of a local area network (LAN) segment, CBIS enabled workstations, a CBIS Enrollment Workstation (CEW), a CBIS Security Manager/Key Processor (CSM/KP), and Information Server. The CBIS Security Monitor ensures configuration management, alerting security personnel of any detected deviation from the security policy. [Ref. 15]

TOP LEVEL ARCHITECTURE

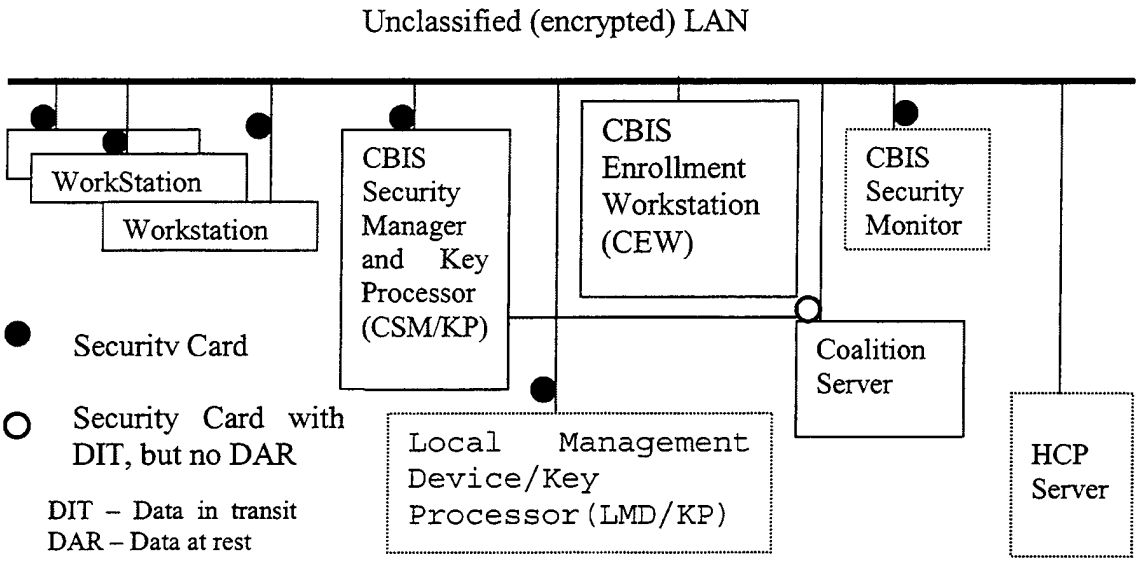


Figure 5.1. CIBS LAN Segment from Ref. [15]

The Security Card, shown below in figure 5.2, is the crucial component used to implement the CBIS system and can be inserted into any computer that has an available PCI slot. The security card, in conjunction with Electronic Document Marking System (EDMS) software, allows Publishers to encrypt documents using algorithms and keys based on the document's classification, releasibility and dissemination controls [Ref. 15 p. 2-1]. Theoretically, the security card is embedded into a workstation connected to a LAN and can share sensitive information across a LAN or WAN securely because the information is protected using embedded encryption and exchanged by matching document and user protection attributes. The Security Card transmits the DoD standard common access card user identification certificate and biometrics to the CBIS Security Manager/Key Processor; performs selected key management functions; and encrypts and

decrypts all information to/from the network and to/from the local storage devices. [Ref. 15 p. 2-2]

Access to the CBIS workstations is granted based on a strong 2-factor authentication – fingerprint and a Common Access Card User Identification Certificate. A third factor is added to this I & A function, that of authorization. User's attributes contain the role-based permissions that form the basis for key/algorithm selection. Access to information at different security and releasibility levels is granted according to these user attributes. All identification, authentication and authorization functions are performed in the Security Manager/Key Processor. [Ref. 15 p. 2-3]

The role-based permissions attributed to users are Author, Publisher/Foreign Disclosure Officer/Foreign Disclosure Representative, Reader, and system administrator. Table 5.1 summarizes the Reader, Author, and Publisher Roles.

Role	Function	Permissions
Reader	Accesses information in the CBIS System and Coalition Server	Read – Coalition Server
Author (Knowledgeable in security policy and procedures)	Drafts, Marks, and adds information into Publisher Review area. Can delete information he/she authored	Read – Coalition Server Write – Publisher Review Area Delete - Publisher
Publisher (Knowledgeable in foreign disclosure policy)	Reviews information to determine if it meets predetermined releasibility criteria for confidentiality, and if it can be moved from Publisher Review area to the Coalition Server. Adds and deletes information in the Coalition Server that he/she published. Reviews information that does not meet the predetermined disclosure criteria, but are nonetheless the subject of a release request	Read/Write/Delete both Coalition Server and Publisher Review Area

Table 5.1. CBIS System Roles and Functions from Ref. [15 p. 2-4]

An author generates or modifies information, properly marks it with the correct sensitivity label and posts information to the Publisher Review Area using a web browser. When the information is uploaded to the Publisher Review Area an alert is automatically sent to the Publisher notifying him of the event. If any modifications need to be made to the information prior to release to the Coalition Server, the Publisher notifies the Author to make changes and re-post. When the information is satisfactory the Publisher releases it to the Coalition Server and it is deleted from the Publisher Review Area. Figure 5.2 shows the Author and Publisher information posting process.

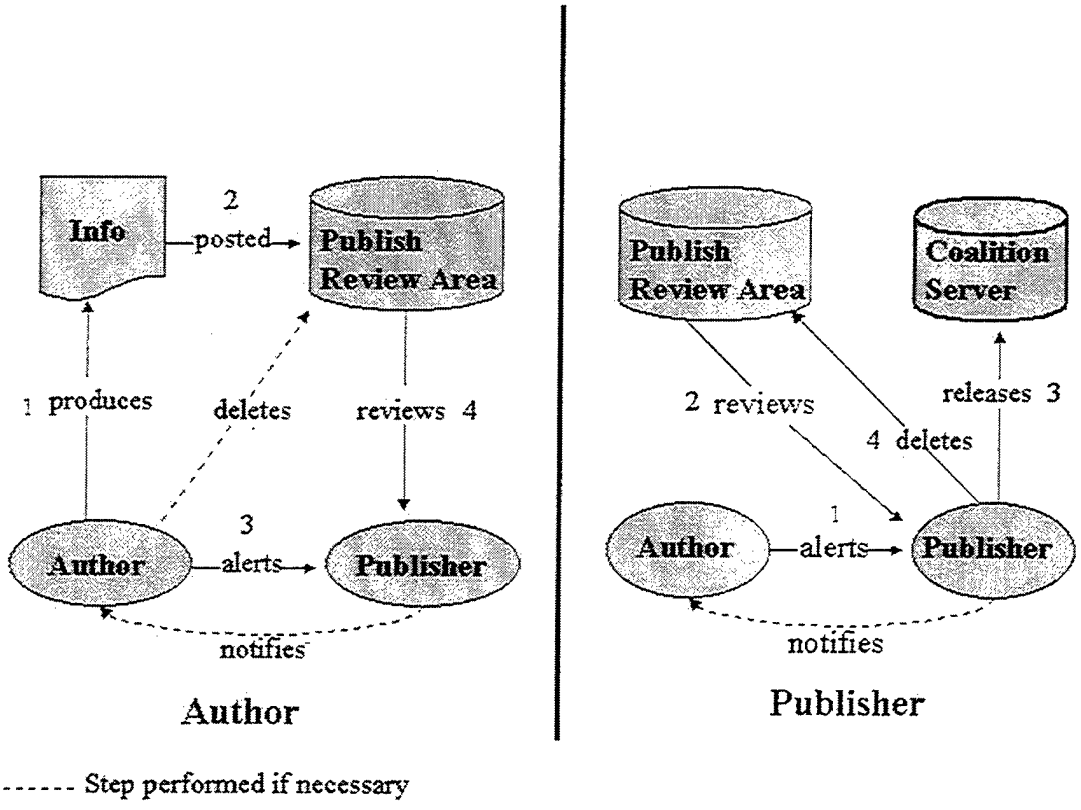


Figure 5.2. Information Posting Process by an Author and Publisher. From Ref. [15]

Users interface with the CBIS Server by way of a Secure Socket Layer (SSL) session to the CBIS homepage. The venue is a type of web search results page. The Coalition Server verifies user authorization when the SSL is established.

a. Summary, pros and cons

Conceptually, the CBIS system is moving coalition information exchange in the right direction. It provides information to the entire coalition in a consistent manner. Intensive training is required for Authors and Publishers to perform their roles. While the training results in a more productive and security conscious worker, the time it takes may require lead-time the coalition may not have. One of the marks of a good secure system is ease of use so that user implementation is not burdensome and becomes second nature. In this area CBIS needs improvement.

Because information is protected based on content rather than by an underlying protection mechanism, one must assume that the information released to the Coalition Server is at a common disclosure level. However, there is no guarantee that this is so. The system can be subject to stenographic attacks in which malicious objects are hidden within a legitimate document or graphic. While a common disclosure level is satisfactory at many levels, some missions may require sharing higher sensitivity level data with specific coalition partners. CBIS should use a trusted computing base system implementing multilevel security to enable a broader sharing of information. This would also enhance the system integrity by providing assurance that the server has been tested for correct security policy enforcement. Another solution to the common disclosure problem could be to establish Author and Publisher interfaces at each security level.

The CBIS system provides an excellent Concept of Operations that describes the system, user roles, and system management responsibilities. It also provides a comprehensive strategy for deployment of the system in small-scale and large-scale coalition contingency.

2. Coalition Data Server

The Coalition Data Server (CoDS) is a multilevel secure web server that can be fully integrated into an existing web environment or used as a stand-alone server. The sensitivity levels that enable file sharing are fully configurable and determined by local coalition policy. Access control and downgrade permissions are auditable. CoDS is built on a B1 or higher rated trusted operating system and complies with U.S. information technology standards. User access is based on the most current version of DoD Public Key Infrastructure Certificates and client Internet Protocol addresses. A marking scheme generated through coalition consensus is used to label hypertext markup language (HTML) documents. Web logging and activity report generation offer an auditing capability. Virus and "dirty word" checks are automatically performed on all uploaded and downgraded documents. [Ref. 16]

Similar to the CBIS system, CoDS uses three information access permissions, Reader, Poster, and Releaser. The Reader is restricted to viewing only those documents that he has clearance and need to know, which are assigned as his user attributes based on individual clearance and functional assignments. A Reader authorized U.S. Secret access may read U.S. Secret data and Coalition releasable data. Similarly, any coalition member authorized Reader access is authorized access to his individual nation's sensitive data

(based on individual national clearance and need to know criteria) and may read Coalition releasable data.

The multilevel security application in CoDS enforces the no write down rule of the Star Property with regard to Poster's privileges. For example, a NATO user with post rights may write data to the NATO Secret compartment but may not write directly to the Coalition releasable compartment, as this would be a downgrade. However, a user with Release rights executes as a trusted subject and is authorized to downgrade information and move it from a higher sensitivity compartment to a lower sensitivity compartment. [Ref. 16] Figure 5.3 is a notional illustration of CoDS.

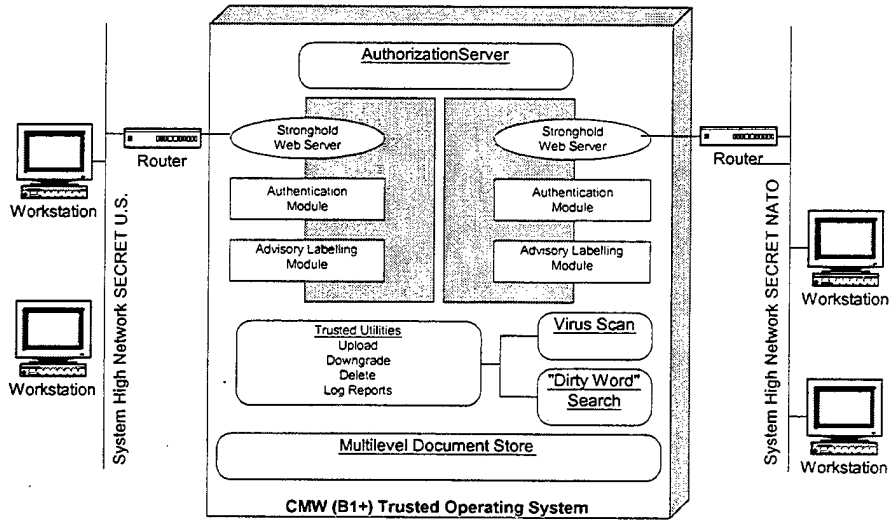


Figure 5.3 Coalition Data Server Architecture. From Ref. [16]

a. Summary, Pros and Cons

The Coalition Data Server is a fully funded acquisition program managed by PMW-161. It has been deployed on the USS Mount Whitney, the U.S. Second Fleet Command Ship, and to Commander, Strike Force Atlantic Headquarters. It has passed several operational tests and is the system of choice with which to exchange information

with coalition maritime forces. This system, however, can be applied throughout the battlespace and is not limited to maritime support. Implementation of multilevel security ensures that the information is not a one size fits all commodity and the use of DoD PKI resolves many authentication and nonrepudiation concerns. The web browser aspect of the implementation makes the user feel at ease operating the system because practical experience has made them comfortable with that interface.

A disadvantage is that as a web-based server it is not a conduit for real-time use. It is a good solution for planning and coordination as long as there is no hard time constraint or urgency involved in communication, for example, the time constraint of getting sensor information to a shooter for immediate targeting. Latency is not an issue with CoDS. A second concern is that the system is hosted on a low assurance platform and is thus subject to potential penetration and system subversion.

3. Joint Coalition Interoperability Integrated Alliance Network

Defense Information Systems Agency and MITRE Corporation have collaborated to provide a solution to coalition system interoperability problems experienced at Allied Combined Air Operations Centers (CAOC). The problem stems from required information residing on the U.S. Secret network where allied operators and decision makers cannot access the information for planning and execution purposes. In the past, providing access to the allies required downgrading the information to NATO or Coalition Releasable, transferring it from the SIPRNET to a floppy disk, and uploading it to the NATO/Coalition LAN. This "air gapping" process was inefficient, time consuming, and required troubleshooting at times. The Joint Coalition Interoperability Integrated Alliance Network seeks to automate the air gapping process by implementing

various multilevel security and filter guard solutions. These technologies enable various data flows such as command and control, intelligence, track, imagery, cartographic, weather, battle assessment, and collaboration. Although complete analysis of the JCIIAN security architecture is beyond the scope of this thesis, below is a discussion of the guards that are part of this network.

a. Command and Control Guard (C2G)

The Command and Control Guard (C2G) supports high-to-low and low to-high text and structured data transfer. Data flows are controlled using an automated filter (configurable to enforce local security policy). An individual authorized to review error files takes action on data that the filter rejects, either manually overriding the C2G decision, deleting the file, or returning the file to the high side for further disposition. The C2G only accepts formatted messages such as the National Imagery Transmission Format (NITF), Air Tasking Orders (ATO's), and Over-the-Horizon (OTH) Gold Messages. As with previous architectures, the danger of steganography is ever-present due to the lack of integrity mechanisms to ensure non-modification of data with the high-side network.

b. Radiant Mercury

Radiant Mercury is similar to the C2G in that it passes classified formatted data between high and low systems using an automated, configurable filter. Radiant Mercury version 3.3, however, will also sanitize, downgrade, disseminate and transliterate messages at differing levels of classification. When data passes into Radiant Mercury, it is parsed and sanitized using specific sanitization rule sets. Based on those same rule sets, the data is sanitized again for each address destination. Then it is

reformatted into the correct format required for each recipient. From there the data is passed into a guard that verifies the sanitization against the release constraint rules. Data is then downgraded as required and passed to each recipient. [Ref. 13 B-3] Here again because the filters are not intelligent the information is vulnerable to steganography attacks.

c. Imagery Support Server Environment (ISSE) Guard

The Imagery Support Server Environment Guard is comprised of a Common Guard Interface (CGI) application and Guard. The CGI allows high side users to encapsulate, label, and transfer their files to the Guard, which validates the encapsulation format, classification labels, and origin and destination hosts. While the Guard checks the "packaging" of the file it does not check the content. The CGI, however, supports "plug in" validation tools to allow reviewing, filtering and dirty word checking. Some of the formats the ISSE Guard accepts include SMTP/MIME compliant e-mail, NITF imagery, gif, text, web pages and database exports. [Ref. 13 p. B-5]

d. Standard Mail Guard (SMG)

The Standard Mail Guard is an NSA accredited guard that controls e-mail traffic between various networks. It can be used to transfer e-mail between high and low side networks more expediently than the ISSE Guard. The guard application employs a filter that can allow or disallow information flow between the high and low networks based on configurable security policy. The originator places a label on an attachment prior to transmitting the e-mail. The SMG then verifies the label against the releasibility policy, rejecting any e-mail that does not meet the criteria. [Ref. 13 p. B-11]

e. Summary, Pros and Cons

The Joint Coalition Interoperability Integrated Alliance Network is a proposed network that continues to undergo testing, certification and accreditation. When accredited and deployed, it should provide most of the qualities a Coalition Task Force Commander will require. Through the C2G and Radiant Mercury it provides the real time operational and tactical data required to create a common operating picture, while the ISSE Guard and SMG provide collaborative tools. There are two pieces missing that would complement the technology discussed and complete the collaborative portion of the network - a web browser, and VTC/white boarding capabilities. The current plan is to integrate a secure web browser, the Trusted Computer Solutions (TCS) Web Guard, into the network when it completes its Beta testing, certification and accreditation process. No plan to integrate VTC or other video based collaboration tools are planned. Although the mission of the system is to support Allied Combined Air Operation Centers, that mission could easily be expanded to meet overall coalition network needs.

C. THE MULTINATIONAL INTEROPERABILITY COUNCIL

The Multinational Interoperability Council was formed to addresses the core issues affecting coalition interoperability such as policy, doctrine, planning, and networking. The six-member council is composed of high ranking military representatives from the United Kingdom, Canada, France, Germany, Australia, and the United States. Commencing in October 1999 the council has met annually to identify the most pressing interoperability issues and assign those issues to a Multinational Interoperability Working Groups for research and recommended resolution. In 1999 some topics addressed were:

- Lead Nation Concept – refine the NATO defined "Lead Nation" concept (similar to that discussed in Chapter II) to apply to all coalition operations
- Information Sharing – National releasibility and disclosure rules are a barrier to coalition information sharing
- Doctrine and Procedures – Accepted applicable NATO doctrine as governing doctrine and policy in future coalition operations
- Coalition Networking – Agreed that development of a Combined Wide Area Network (CWAN) would pose an interim solution to information exchange problems

In November of 2000 the MIC met again to follow up on issues raised at the last meeting and developed new action items:

- All Council members adopted a Lead Nation Concept Point Paper and it was agreed that the each Member nation should consider possible inclusion of the Lead Nation concept into national/allied doctrinal documents.
- NATO Doctrine to be reviewed by Non-NATO nations for acceptability and applicability

An Information Exchange Requirements template should be adopted to stimulate thought regarding what information sharing was required. Both the U.K and Australia have established separate templates that are under national consideration/revision. Rules of releasibility should be developed by each nation to enhance exchange of information in a coalition environment.

D. SUMMARY

This chapter has introduced just a few of the systems deployed and in development to provide the coalition connectivity and information sharing required in warfighting today. While it would be nearly impossible for any one system to meet all the operational requirements of the Coalition Joint Force Commander, the systems discussed come close to meeting user requirements. However, warfighters, scientists and engineers must guard against stovepiped development of C4I systems. Of the systems discussed, CBIS is the only system whose concept of operations broadly includes

meeting any mission. CoDS is a Navy sponsored program designed to provide partial solutions to Navy coalition interoperability problems. Although it can be used as a *joint* interoperability solution the CoDS CONOPS does not address these uses. The Joint Coalition Interoperability Integrated Alliance Network supports air operations specifically, although it too can support other operations that are not addressed in the concept of operations. It is unlikely that the other services are aware of the C4I solutions being forwarded by each branch. With each service branch vying for development dollars to solve coalition interoperability problems, one can only hope that the competition will breed cooperation, the sharing of innovative ideas and technology for the common good.

VI. CONCLUSIONS AND RECOMMENDATIONS

A. SUMMARY

U.S. national strategy and doctrine reflect an intention and preference to conduct military operation in a coalition environment. As coalition partners assume greater responsibility and risk in the battlespace the requirement to exchange information increases in order to synchronize operations and prevent blue on blue engagements. Planning and execution of multinational operations rely on strong communications and collaboration best achieved though network interoperability. One of the most significant barriers to coalition network interoperability is establishing information protection measures and policy to enforce multilevel security. While the U.S. and its allies and friends develop network security solutions, a balance must be struck between developing one system that "does it all" and several individual systems that offer specific stovepiped solutions.

B. CONCLUSIONS AND RECOMMENDATIONS

Several conclusions can be drawn from this study. These conclusions will be followed by recommendation for improvement.

1. Planning for Unanticipated Coalition Operations is Difficult

Because the need for a coalition military operation arises rapidly, time is a critical factor in campaign and mission planning as well as troop and essential equipment deployment. Although regional contingency plans exist that include, or can be modified to include, coalition operations, operational plans cannot always predict the actual situational crisis. At these times, network communications become a critical enabler by providing collaboration tools for operational and strategic planning. Video

teleconference with white board capabilities can render unnecessary a time consuming trip to a central location for multinational commander's planning meetings. Consensus can be derived during the teleconference with hardcopy messages to follow-up on decisions.

a. Recommendation

Establishing a Regional Coalition Information Grid (RCIG) should be explored by the Commander in Chief of each region. Such an information grid would provide a secure network on which to conduct contingency planning, military exercises, peacekeeping operations and wartime communications. Each Regional Coalition Information Grid would incorporate data released from various national eyes-only systems within the region. Together the RCIGs form an overarching Coalition Information Grid, which in turn is a sub set of the Global Information Grid. Figure 6.1 illustrates the Coalition Information Grid concept. Both the regional and global information grids must share a common document marking and labeling policy with regard to sensitivity terminology. Another security issue that requires coordination and consensus is the Public Key Infrastructure Certificate Authority role and how to issue and revoke certificates. Finally, each nation would have to struggle with assessing the value of their military information and evaluate to what extent it can be shared within the region and on a global scale while maintaining some semblance of assurance that the information will remain protected from unauthorized disclosure

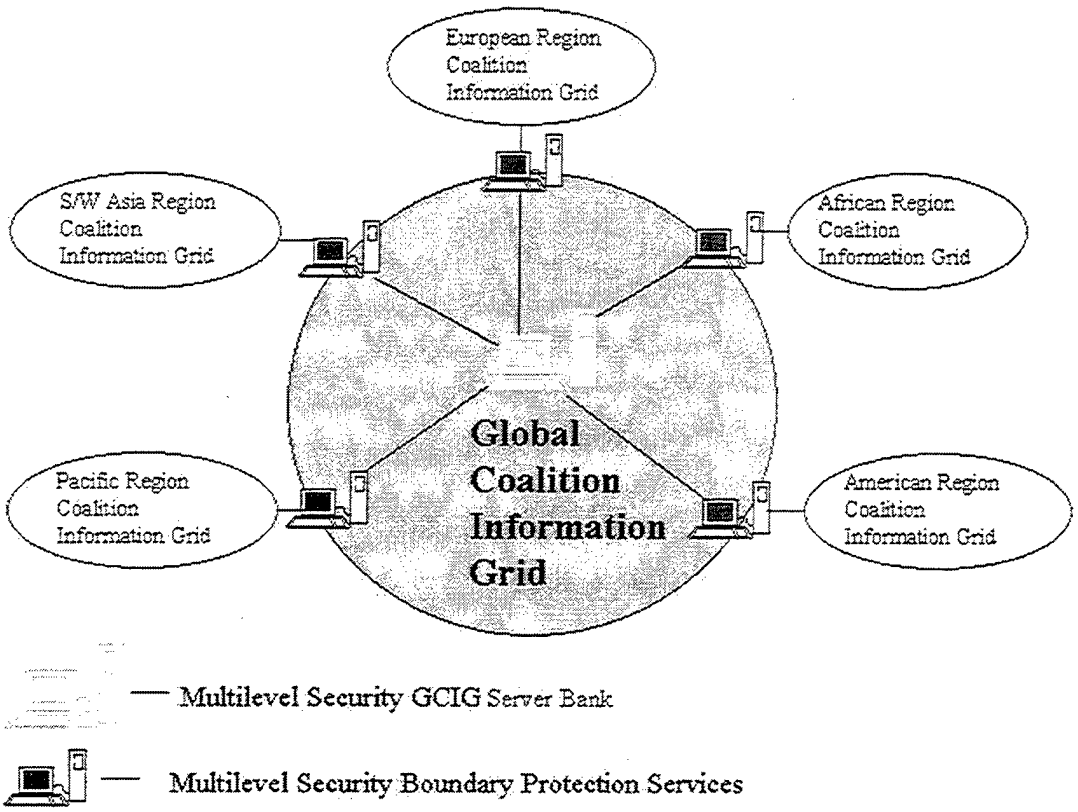


Figure 6.1 Global and Regional Coalition Information Grid

2. Common Standards Encourage Interoperability

Encouraging development of systems that conform to internationally accepted standards is a good way to plan for future coalition operations. In addition to information systems compatibility, developing a concept of network operations, common security practices and goals, and standard operating procedures prior to hostilities, could smooth the friction caused by forming coalitions. These provide a framework and guidance on which to plan and execute these operations. The work being performed by the Multinational Interoperability Working Groups and Council in partnership with the Combined Communication and Electronics Board will further the establishment of these standards.

a. Recommendations

While the work being conducted by the Multinational Interoperability Council will further the cause for coalition interoperability; the focus of the council's interoperability resolution efforts seem to be on the Eurasian Continent. Expanding the membership of the council to include representatives from the Pacific Rim and Southwest Asia nations such as Japan, South Korea and Saudi Arabia add a more global perspective to the Council. If this is unacceptable, perhaps each region should establish a Multinational Interoperability Council for that region. These regional councils could focus on developing the doctrine, policy, network architecture and training specific to that region. Perhaps, on an annual basis, all the councils can gather for a symposium to share progress reports or introduce new technology/innovative concepts.

A second recommendation is for the U.S. military and the Multinational International Council to look to institutions of higher learning within their own nations to help wrestle with and provide solutions to the problems. For example, the Naval Postgraduate School (NPS) in Monterey California is uniquely qualified to render assistance for the following reasons:

- Students from all branches of the Armed Forces
- International students
- Distinguished faculty members
- Advanced classified/unclassified computer laboratories
- Center for Excellence and Executive Education
- Experienced people who have wrestled with the problem

Members of the Multinational Interoperability Working Groups (MIWG) are

assigned these duties in addition to their primary duties. Developing a partnership with the NPS may assist them in performing their collateral MIWG duties as well as solicit new ways of thinking about the problem. For instance, after an annual meeting of the Multinational Interoperability Council, the MIWG can recruit thesis students to work on action items. In this way the student works on a pertinent, militarily relevant topic and the MIWG is provided with a thoroughly researched study with recommendations or even solutions.

Using the above discussion as a springboard, a third recommendation is for the NPS to heighten the student's awareness of coalition issues through incorporating them into their curriculum. The relevance of the coalition interoperability problem cuts across several of the academic departments.

- National Security Affairs – explore coalition interoperability policy and cultural issues
- C4I – explore coalition organizational structure and systems integration issues
- Computer Science – explore coalition network security policy and implementation; computer network attack and defense
- Information Systems – explore coalition system connection, interface and architecture
- Information Warfare – explore coalition information operation collaboration
- Systems Management – explore coalition logistics, transportation, and system acquisitions
- Modeling Virtual Environment Simulation – explore coalition modeling and simulation

These are only a few examples of incorporating coalition studies into the NPS curriculum. It would be extremely beneficial for the respective U.S. service branches and international militaries for their students to return to their military duties with an

appreciation for coalition operations and innovative ideas to resolve some of the key issues.

3. Solutions Without Requirements

Several technologies are being forwarded as partial solutions to facilitate coalition network operations without benefit of a Mission Needs Statement or Operational Requirements Document. The systems summarized in the previous chapter were also developed absent of these documents, however, the security policies incorporated by all were based on Department of Defense Information Security Directives. Be that as it may, developing systems absent of requirements may result in building an incomplete solution that complies with security directives. Capabilities and functionality must be defined in order to design the right system. This thesis has identified the need of information exchange and collaboration capabilities, as well as the ability for systems to understand each other, a common network operation plan and standard operational procedures. These are the minimal requirements necessary to meet the network needs of the coalition commander. Several CINCs list the need for coalition interoperability and information sharing in their Integrated Priority Lists (IPLs) and After Action Reports (AAR) but have not directed that they be codified in a Mission Needs Statement. [Ref. 13 p. 1-1] Until such time as these needs are justified in Mission Needs Statements and Operational Requirements Documents systems will continue to be developed with out benefit of all user requirements. Of course it is unrealistic to assume that one system could be built to achieve the interoperability and security requirements of coalitions. However, the possibility exists that, absent user requirements, systems offered as solutions may be too narrow in focus and result in stovepiped systems.

a. Recommendation

Each regional CINC should submit Coalition Wide Area Network (CWAN) requirements, as a Mission Needs Statement, through their chain of command. These MNS should then be forwarded for review by the Combined Communications and Electronics Board. The CCEB should act as an Executive Agent to ensure all regional CWANs are developed with interoperability among CWANs in mind.

C. AREAS FOR FURTHER STUDY

Although coalition interoperability encompasses more than protecting network operations, much more study within this area is required:

- Extending the secure CWAN to the unit and "man in the field" level
- Protecting and sharing the sensor-to-shooter information flow
- Generating and implementing a coalition document labeling scheme
- Feasibility of constructing regional and global coalition information grids
- Automating a releasibility mechanism that incorporates a wizard like application that walks the releaser through the releasibility security policy [Ref. 13 p. 19]
- Transposing recent military operation's Lessons Learned into Mission Needs Statements

There is a plethora of work that requires attention in the coalition warfare environment. If decomposed to its essential elements each problem may be more surmountable. Solutions to the challenge of providing a secure network for coalition operations is within our grasp and can be achieved given the courage and commitment from leadership to see the task through to completion.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Grause, K., Morley, P. Odell, R.R., and Ruiz-Ramon, F., *Toward a U.S. Navy Strategy for C4I Interoperability with Allies,* Center for Naval Analyses, June 1999.

2. Joint Pub 1-02, "Department of Defense Dictionary of Military and Associated Terms", March 1994.

3. Joint Pub 3-16, "Joint Doctrine for Multinational Operations", April 2000.

4. Joint Doctrine Encyclopedia, July 1997.

5. Gangemi, G.T., Russell, D., *Computer Security Basics*, O'Reilly & Associates, Inc. 2001.

6. Naval Postgraduate School, Center for Information Systems Security Studies and Research, "Introduction to Computer Security", Winter 2000, copyright 1998.

7. Bell, D., and La Padula, L "Secure Computer Systems: Mathematical Foundations and Model.", MITRE Report, MTR 2547 v2, November 1973.

8. Biba, K., "Integrity Consideration for Secure Computer Systems." U.S. Air Force Electronic Systems Division Technical Report 76-372, 1977.

9. Common Criteria Editorial Board. *Common Criteria for Information Technology Security Evaluations*, version 0.6, April 1994.

10. Personal communications. Telephone conversation between Susan McGovern and Andrew J. Blank, Principle Scientist Communications Division NATO C3 Agency, April 2001.

11. Alberts, D.S., Garstka, J.J., Stein, F.P., C4ISR Cooperative Research Program (CCRP), *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd edition (Revised).

12. Defense Information System Agency, "Multilevel Security in the Department of Defense: The Basics", from http://nsi.org/Library/Compsec/sec1.html, available through the DoD MLS Program; March 1995.

13. Dowell, S. and Yuan, A., "Joint Coalition Interoperability Integrated Alliance Network Proposal Multiple Security Levels Technical Solution Description" MITRE Corp, for Defense Information Systems Agency Center for Information Assurance Engineering Communication Security Engineering Division, Draft Report February 2001.

14. Sterne, D.F., "On the Buzzword 'Security Policy'" as printed in IEEE Computer Society Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos, May 1991.

15. Joint Forces Command, "Content-Based Information Security Concept of Operations (CONOPS), Version 2.0, January 2001.

16. Space and Naval Warfare Center, Naval Research Laboratories "Coalition Data Server, System Security Authorization Agreement", January 2000.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Road, Suite 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, CA 93943-5101

3. Carl Siel 1
   Space and Naval Warfare Systems Command
   PMW 161
   Building OT-1, Room 1024
   4301 Pacific Highway
   San Diego, CA 92110-3127

4. Commander, Naval Security Group Command 1
   Naval Security Group Headquarters
   9800 Savage Road
   Suite 6585
   Fort Meade, MD 20755-6585

5. Ms. Deborah M. Cooper 1
   Deborah M. Cooper Company
   P.O. Box 17753
   Arlington, VA 22216

6. Ms. Louise Davidson 1
   N643
   Presidential Tower 1
   2511 South Jefferson Davis Highway
   Arlington, VA 22202

7. Mr. William Dawson 1
   Community CIO Office
   Washington DC 20505

8. Capt. James Newman 1
   N64
   Presidential Tower 1
   2511 South Jefferson Davis Highway
   Arlington, VA 22202

9. Mr. Richard Hale 1
Defense Information Systems Agency, Suite 400
5600 Columbia Pike
Falls Church, VA 22041-3230

10. Ms. Barbara Flemming 1
Defense Information Systems Agency, Suite 400
5600 Columbia Pike
Falls Church, VA 22041-3230

11. LCDR Ed Bryant 1
Defense Information Systems Agency, Suite 400
5600 Columbia Pike
Falls Church, VA 22041-3230

12. Mr. Arison 1
JCS/J6
Pentagon
Washington, D.C. 20350-2000

13. Capt Maslowsky 1
CNO/N62
Pentagon, Washington D.C. 20350-2000

14. LT Susan C. McGovern 1
7848 Gladwater Road
Falcon, CO 80831

15. Dr. Orin Marvel, CC 1
Naval Postgraduate School
589 Dyer Road
Monterey, CA 93943-5103

16. Dr. Cynthia E. Irvine, CS 1
Naval Postgraduate School
589 Dyer Road
Monterey, CA 93943-5103

17. Chair, Code CC 1
Naval Postgraduate School
589 Dyer Road
Monterey, CA 93943-5103